目　录

《俄罗斯数学教材选译》序

前　言

第 1 章　群论的构造 1
§1　小维数的典型群 1
1. 一般概念 1
2. 群 SU(2), SO(3) 的参数化 2
3. 满同态 SU(2) → SO(3) 4
4. 群 SO(3) 的几何表示 6
5. 四元数 6
习题 9
§2　子群的陪集 10
1. 初等性质 10
2. 循环群的结构 12
习题 13
§3　群在集合上的作用 14
1. $G \to S(\Omega)$ 的同态 14
2. 轨道和点的稳定子群 14
3. 群作用在集合上的例子 16
4. 齐次空间 19

习题 20
§4 商群与同态 21
1. 商群的概念 21
2. 群的同态定理 23
3. 换位子群 26
4. 群的积 27
5. 生成元与定义关系 29
习题 33

第 2 章 群的结构 36
§1 可解群与单群 36
1. 可解群 36
2. 单群 38
习题 41
§2 西罗 (Sylow) 定理 42
习题 47
§3 有限生成交换群 47
1. 例子和初步结果 47
2. 无挠交换群 49
3. 有限秩的自由交换群 51
4. 有限生成交换群的结构 53
5. 分类问题的其它方法 54
6. 有限交换群的基本定理 57
习题 60
§4 线性李群 60
1. 定义和例子 60
2. 矩阵群中的曲线 62
3. 同态的微分 64
4. 李群的李代数 65
5. 对数 66
习题 67

第 3 章 表示论基础 68
§1 线性表示的定义和例子 71
1. 基本概念 71
2. 线性表示的例子 75
习题 79

§2 酉性和可约性 80
1. 酉表示 80
2. 完全可约性 83
习题 85
§3 有限旋转群 86
1. SO(3) 中有限子群的阶 86
2. 正多面体群 88
习题 91
§4 线性表示的特征标 92
1. 舒尔 (Schur) 引理和它的推论 92
2. 表示的特征标 94
习题 99
§5 有限群的不可约表示 99
1. 不可约表示的个数 99
2. 不可约表示的维数 101
3. 交换群的表示 103
4. 某些特殊群的表示 105
习题 107
§6 群 SU(2) 和群 SO(3) 的表示 109
习题 112
§7 表示的张量积 112
1. 逆步表示 112
2. 表示的张量积 113
3. 特征标环 114
4. 线性群的不变量 117
习题 121

第 4 章 环. 代数. 模 123
§1 环论构造 123
1. 环的理想及商环 123
2. 多项式的分裂域 125
3. 环的同构定理 128
习题 130
§2 关于环的一些结果 130
1. 高斯整数 130
2. 两个平方之和的标准分解 132
3. 唯一因子分解环的多项式扩张 133

4. 乘法群 U(Z_n) 的结构 134
习题 138
§3 模 139
1. 关于模的初步知识 139
2. 自由模 142
3. 环的整元素 145
习题 146
§4 域上代数 146
1. 代数的定义及例子 146
2. 可除代数 (体) 149
3. 群代数及它上的模 152
习题 159
§5 李代数 $\mathfrak{sl}(2)$ 上的不可约模 160
1. 起初的材料 160
2. 权及重数 162
3. 最高权向量 163
4. 分类的结果 164
习题 165

第 5 章 伽罗瓦理论初步 166
§1 域的有限扩张 166
1. 本原元素和扩张的次数 166
2. 分裂域的同构 170
3. 本原元素的存在性 172
习题 173
§2 有限域 173
1. 存在性和唯一性 173
2. 有限域的子域及自同构 175
3. 默比乌斯 (Möbius) 反演公式及其应用 176
习题 180
§3 伽罗瓦对应 182
1. 初步结果 182
2. 基本的伽罗瓦对应 184
3. 伽罗瓦对应的例证 186
习题 188

§4 伽罗瓦群的计算 189
1. 群 Gal(f) 在多项式 f 的根上的作用 189
2. 素数次多项式及素数次群 191
3. 以模 p 简化的方法 193
4. 正规基 197
习题 200
§5 伽罗瓦扩张及相近的问题 200
1. 算术级数中的素数 200
2. 伽罗瓦群为交换群的扩张 201
3. 范数与迹 202
4. 循环扩张 205
5. 方程可用根式解的判别法 207
习题 210
§6 有限群中的刚性和有理性 210
1. 定义及基本定理的表述 210
2. 解的计算 212
3. 刚性的例子 214
习题 215
§7 结束语 216

附录　未解决的问题 218
1. 有限单群的分类 218
2. 正则自同构 219
3. 奇异李代数 219
4. 伯恩赛德 (Burnside) 问题 219
5. 多项式自同构的有限群 220
6. 单可约群 220
7. 伽罗瓦逆问题 221

习题的答案与提示 223

教学法方面的意见 232

考试题　(没有特征标理论) 233

高等代数课程教学大纲　(第三学期, 1995 年) 235

表示论的例证材料 236

名词索引 239

第 1 章　群论的构造

本章展开在 [BA I] 第 4 章中引入的群的概念. 首先指出的是, 我们这里注重的不是抽象群, 那是属于许多专业课程的事, 而是用于了解各种自然的群的 "作用". 正是各种具体的群的实现推动了一般群论的发展, 并树立了它为有益的数学研究工具的声望. 以一些个别的 (但也是重要的) 例子为背景研究群同态 (群的满同态、群的同构) 以及群论构造的想法变得更加迫切. 这使我们能够将复杂的研究对象变得更简单.

§1 小维数的典型群

1. 一般概念　线性代数和几何教程给我们提供了新的群的范例, 这些范例值得较详细的谈谈. 在仿射空间、欧几里得空间、埃尔米特空间和辛空间中保留一个固定点 (譬如, 坐标原点) 不变的变换群中分离出一些子群, 由此产生了那些称之为典型群的 $\mathrm{GL}(n), \mathrm{SL}(n), \mathrm{O}(n), \mathrm{SO}(n), \mathrm{U}(n), \mathrm{SU}(n), \mathrm{Sp}(n)$. 我们指出, 它们在李群中真正的地位已在 [BA II] 中提到, 同时将要在第 2 章简要的论述. 我们并不打算全面地描写典型群的性质, 那是其它书的任务. 在 n 不大的情况下, 我们称典型群是小维的. 对于群 $\mathrm{GL}(n), \mathrm{SL}(n)$, 我们在前面已经遇到过 (见 [BA I]). 为了回避对几何的较大依赖性, 人们在空间中选择了标准正交基, 并由此产生了正交群和酉群的矩阵形式的等价定义:

$$\mathrm{O}(n) = \left\{A \in M_n(\mathbb{R}) | {}^tA \cdot A = A \cdot {}^tA = E\right\},$$

$$\mathrm{SO}(n) = \{A \in \mathrm{O}(n) | \det\ A = 1\},$$

$$\mathrm{U}(n)=\{A\in M_n(\mathbb{C})|A^*\cdot A=A\cdot A^*=E\},$$
$$\mathrm{SU}(n)=\{A\in \mathrm{U}(n)|\det\ A=1\}.$$

其中 $A^*=\overline{{}^tA}$ 为 $A=(a_{ij})$ 的转置矩阵并将元素 a_{ij} 用其复数共轭 $\overline{a_{ij}}$ 代替所得的矩阵. 群 $\mathrm{SL}(n),\mathrm{SO}(n),\mathrm{SU}(n)$ 分别称为**特殊** (**线性**、**正交**、**酉**) **群**. 特别地,

$$\mathrm{O}(1)=\{\pm1\},\quad \mathrm{SO}(1)=1:=\{1\},$$
$$\mathrm{U}(1)=\left\{e^{i\varphi}|0\leqslant\varphi<2\pi\right\},\quad \mathrm{SU}(1)=1,$$
$$\mathrm{SO}(2)=\left\{\left.\begin{pmatrix}\cos\varphi & -\sin\varphi\\ \sin\varphi & \cos\varphi\end{pmatrix}\right|,\quad 0\leqslant\varphi<2\pi\right\}\cong \mathrm{U}(1).$$

自然对应

$$\begin{pmatrix}\cos\varphi & -\sin\varphi\\ \sin\varphi & \cos\varphi\end{pmatrix}\mapsto e^{i\varphi}$$

是 SO(2) 对应到 U(1) 的一个同构. 因为复数 $e^{i\varphi},0\leqslant\varphi<2\pi$, 的几何表示是 $\mathbb{R}^2$ 中具有单位半径的圆 S^1, 所以人们也称群 SO(2) 与圆 S^1 为**拓扑等价**. 这个术语的真正涵义在几何课程中是清楚的.

群 SO(2) 与 SO(3) 之间的明显的联系要小得多. 我们来初步地讲一讲群 SU(2) 的几何变换, 它将使我们得到群 SO(3) 的几何变换.

2. 群 SU(2), SO(3) 的参数化　由著名的欧拉定理, 三维欧几里得空间 $\mathbb{R}^3$ 的正常旋转的群 SO(3) 的每个元素是围绕某一固定轴的旋转. 譬如说, 矩阵

$$B_\varphi=\begin{pmatrix}\cos\varphi & -\sin\varphi & 0\\ \sin\varphi & \cos\varphi & 0\\ 0 & 0 & 1\end{pmatrix},\quad C_\theta=\begin{pmatrix}1 & 0 & 0\\ 0 & \cos\theta & -\sin\theta\\ 0 & \sin\theta & \cos\theta\end{pmatrix}\tag{1}$$

对应的是围绕轴 Oz 和 Ox 的角度为 φ 和 θ 的两个旋转. 利用欧拉角 φ,θ,ψ $(0\leqslant\varphi,\psi<2\pi,0\leqslant\theta<\pi)$ 的旋转的参数化 (它们的几何意义目前我们暂时不感兴趣), 任意矩阵 $A\in\mathrm{SO}(3)$ 可以写为

$$A=B_\varphi C_\theta B_\psi,\tag{2}$$

这里 $B_\varphi,C_\theta,B_\psi$ 是上面 (1) 中形式的矩阵.

下面令

$$g=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\in\mathrm{SU}(2).$$

则

$$g^*={}^t\bar g=\begin{pmatrix}\overline{\alpha} & \overline{\gamma}\\ \overline{\beta} & \overline{\delta}\end{pmatrix},\quad g^{-1}=\begin{pmatrix}\delta & -\beta\\ -\gamma & \alpha\end{pmatrix}.$$

因为 $g \in \mathrm{U}(2) \Longleftrightarrow g^* = g^{-1}$, 所以 $\delta = \overline{\alpha}, \gamma = -\overline{\beta}$. 于是, 对于任意 $g \in \mathrm{SU}(2)$ 有

$$g = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}, \quad |\alpha|^2 + |\beta|^2 = 1. \tag{3}$$

反之, 如果 g 是形如 (3) 的矩阵, 那么显然 $g \in \mathrm{SU}(2)$. 因此群 SU(2) 中的每个元被满足 $|\alpha|^2 + |\beta|^2 = 1$ 的复数对 α, β 唯一确定. 如果令 $\alpha = \alpha_1 + i\alpha_2, \beta = \beta_1 + i\beta_2$, 其中 $\alpha_k, \beta_k \in \mathbb{R}, i = \sqrt{-1}$, 那么条件 $|\alpha|^2 + |\beta|^2 = 1$ 转化为

$$\alpha_1^2 + \alpha_2^2 + \beta_1^2 + \beta_2^2 = 1,$$

于是可以说, 群 SU(2) 拓扑等价 (同胚) 于四维实空间中的球面 S^3.

我们将注意力转移到酉矩阵

$$b_\varphi = \begin{pmatrix} e^{\frac{i\varphi}{2}} & 0 \\ 0 & e^{-\frac{i\varphi}{2}} \end{pmatrix}, \quad c_\theta = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & i\sin\left(\frac{\theta}{2}\right) \\ i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}. \tag{4}$$

正如线性代数教程所证明的 (在所给条件下验证也是直接的), 对于形如 (3) 的酉矩阵 g, 存在酉矩阵 u 使得

$$g = ub_\varphi u^{-1}, \tag{5}$$

其中 φ 由方程 $\alpha_1 = \cos\left(\frac{\varphi}{2}\right)$ 所确定. 同样指出, 对于任意矩阵 (3), 当 $\alpha\beta \neq 0$ 时, 可以有形式

$$a(\varphi, \theta, \psi) = b_\varphi c_\theta b_\psi = \begin{pmatrix} \cos\frac{\theta}{2} \cdot e^{\frac{i(\varphi+\psi)}{2}} & i\sin\frac{\theta}{2} e^{\frac{i(\varphi-\psi)}{2}} \\ i\sin\frac{\theta}{2} \cdot e^{\frac{i(\psi-\varphi)}{2}} & \cos\frac{\theta}{2} e^{\frac{-i(\varphi+\psi)}{2}} \end{pmatrix}, \tag{6}$$

其中①

$$0 \leqslant \varphi < 2\pi, \ 0 \leqslant \theta < \pi, \ -2\pi \leqslant \psi < 2\pi.$$

这只要令

$$|\alpha| = \cos\frac{\theta}{2}, \quad \operatorname{Arg}\alpha = \frac{\varphi + \psi}{2},$$
$$|\beta| = \sin\frac{\theta}{2}, \quad \operatorname{Arg}\beta = \frac{\varphi - \psi + \pi}{2},$$

运用这样的事实: 每个复数 z 有两个实参数 $|z|$ 和 $\arg z$ ($\operatorname{Arg} z$ 是幅角 $\arg z$ 的主值).

现在我们开始解决这一节的主要问题.

---

①后面我们将看到, φ, θ, ψ 就是欧拉角. 酉矩阵 $\pm g$ 对应 $\mathbb{R}^2$ 中的同一个旋转, ψ 的变化范围缩小为半个区间 $[0, 2\pi]$.

3. 满同态[①] $SU(2) \to SO(3)$. 让三维欧氏空间 $\mathbb{R}^3$ 上的每个具有范数 $(\mathbf{x}|\mathbf{x}) = x_1^2 + x_2^2 + x_3^2$ 的向量 $\mathbf{x} = x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + x_3\mathbf{e}_3$ 对应到一个二阶复矩阵

$$H_{\mathbf{x}} = \begin{pmatrix} x_3 & x_1 + ix_2 \\ x_1 - ix_2 & -x_3 \end{pmatrix}. \tag{7}$$

形如 (7) 的矩阵空间 M_2^+ 由所有具有零迹 (${}^t\overline{H}_{\mathbf{x}} = H_{\mathbf{x}}, \mathrm{tr} H_{\mathbf{x}} = 0$) 的埃尔米特矩阵组成, 而且显然向量 $\mathbf{x} \in \mathbb{R}^3$ 与矩阵 $H_{\mathbf{x}} \in M_2^+$ 之间的对应是一一对应. 特别地, 基向量 $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3 \in \mathbb{R}^3$ 对应于基矩阵 $h_k = H_{\mathbf{e}_k}, k = 1, 2, 3$:

$$h_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad h_2 = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \quad h_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}; \tag{8}$$
$$H_{\mathbf{x}} = x_1h_1 + x_2h_2 + x_3h_3, \ M_2^+ = \langle h_1, h_2, h_3 \rangle_{\mathbb{R}}.$$

我们注意到, 在基 (8) 上具有矩阵 A 的 M_2^+ 上的线性算子 $\mathcal{A}^{-1} : H_{\mathbf{x}} \mapsto H_{\mathbf{y}}$ 将对应到在基 e_1, e_2, e_3 上具有同样矩阵 A 的 $\mathbb{R}^3$ 上的所确定的线性算子 $\mathcal{A} : \mathbf{x} \mapsto \mathbf{y}$, 这因为 $H_{\alpha\mathbf{x}} = \alpha H_{\mathbf{x}}, H_{\mathbf{x}+\mathbf{x}'} = H_{\mathbf{x}} + H_{\mathbf{x}'}$. 因为在下面将不使用任何其它的基, 所以我们有时将算子和它们对应的矩阵视为同一的.

现在令 g 是群 $SU(2)$ 的一个固定的元. 来考察映射

$$\Phi_g^+ : H_{\mathbf{x}} \mapsto gH_{\mathbf{x}}g^{-1}. \tag{9}$$

因为相似矩阵的迹相等, 所以 $\mathrm{tr}\Phi_g^+(H_{\mathbf{x}}) = \mathrm{tr}(H_{\mathbf{x}}) = 0$. 此外, $g^* = {}^t\overline{g} = g^{-1}$, 所以

$$(gH_{\mathbf{x}}g^{-1})^* = (g^{-1})^* H_{\mathbf{x}}^* g^* = gH_{\mathbf{x}}g^{-1}$$

从而 $\Phi_g^+(H_{\mathbf{x}}) \in M_2^+$:

$$\Phi_g^+(H_{\mathbf{x}}) = \begin{pmatrix} y_3 & y_1 + iy_2 \\ y_1 - iy_2 & -y_3 \end{pmatrix} = H_{\mathbf{y}},$$

其中 $\mathbf{y} = (y_1, y_2, y_3) \in \mathbb{R}^3$. 由等式 (7) 和 (9) 的定义可见

$$\Phi_g^+(H_{\alpha\mathbf{x}} + \alpha'\mathbf{x}') = \alpha\Phi_g^+(H_{\mathbf{x}}) + \alpha'\Phi_g^+(H_{\mathbf{x}'}).$$

于是, 映射 Φ_g^+ (相应地 Φ_g) 是 M_2^+ 上 (相应地 $\mathbb{R}^3$ 上) 的线性算子.

我们来证明 $\Phi_g : \mathbb{R}^3 \to \mathbb{R}^3$ 是正交算子. 事实上,

$$\begin{aligned}(\Phi_g(\mathbf{x})|\Phi_g(\mathbf{x})) &= (\mathbf{y}|\mathbf{y}) = -\det H_{\mathbf{y}} = -\det \Phi_g^+(H_{\mathbf{x}}) \\ &= -\det gH_{\mathbf{x}}g^{-1} = -\det H_{\mathbf{x}} = x_1^2 + x_2^2 + x_3^2 = (\mathbf{x}|\mathbf{x}),\end{aligned}$$

[①] 作者在 [BA I] 第 126 页指出: "'同态' 一词已有被 '态射' 取代的倾向, 读者应了解这些术语"—— 译者注.

即 Φ_g 保持范数不变, 而且是纯量积. 暂时我们还不知道 Φ_g 是否改变空间 $\mathbb{R}^3$ 的方向, 这取决于 $\det\Phi_g$ 的符号. 我们仅仅知道 $\det\Phi_g=\pm1$. 由定义,

$$\Phi_g^+(\Phi_{g'}H_{\mathbf{x}})=g(g'H_{\mathbf{x}}g'^{-1})g^{-1}=(gg')H_{\mathbf{x}}(gg')^{-1}=\Phi_{gg'}^+(H_{\mathbf{x}}),$$

而且对于 $E=\begin{pmatrix}1&0\\0&1\end{pmatrix}\in\mathrm{SU}(2)$, Φ_E^+ 是 3 阶单位正交矩阵. 于是, 对应

$$\Phi:g\mapsto\Phi_g\quad(\text{或 }\Phi^+:g\mapsto\Phi_g^+)$$

是 SU(2) 到 O(3) 内的同态. 其核由满足 $\Phi_g^+=\Phi_E^+$ 的酉矩阵 g 组成. 换句话说,

$$\begin{aligned}\mathrm{Ker}\Phi&=\{g\in\mathrm{SU}(2)|gH=Hg,\forall H\in M_2^+\}\\&=\{g\in\mathrm{SU}(2)|gh_j=h_jg,j=1,2,3\},\end{aligned}$$

其中 h_1,h_2,h_3 是空间 M_2^+ 的基 (8). 直接验证知

$$g=\begin{pmatrix}\alpha&\beta\\-\overline{\beta}&\overline{\alpha}\end{pmatrix},\quad gh_j=h_jg,\quad 1\leqslant j\leqslant3\Longrightarrow$$
$$\Longrightarrow g=\pm E\Longrightarrow\mathrm{Ker}\Phi=\{\pm E\}.$$

现在我们来看酉矩阵在同态 Φ 下的像. 计算 Φ^+ 在基 (8) 上的表示:

$$\begin{aligned}&b_\varphi h_1b_\varphi^{-1}=(\cos\varphi)h_1+(\sin\varphi)h_2,\\&b_\varphi h_2b_\varphi^{-1}=(-\sin\varphi)h_1+(\cos\varphi)h_2,\\&b_\varphi h_3b_\varphi^{-1}=h_3.\end{aligned}$$

于是 (这里我们自由地由 Φ^+ 过渡到 Φ 且由矩阵过渡到算子), $\Phi_{b_\varphi}=B_\varphi$ (见 (1)) 是三维欧氏空间 $\mathbb{R}^3$ 绕轴 Ox_3 (或 h_3) 的转角为 φ 的旋转. 如果选择 φ 和 u 满足关系 (5), 那么由于 Φ 是同态, 我们有

$$\Phi_g=\Phi_u\Phi_{b_\varphi}\Phi_u^{-1},\det\Phi_g=\det\Phi_u\cdot1\cdot(\det\Phi_u)^{-1}=1.$$

这表明, 实际上 Φ 是 SU(2) 到 SO(3) 内的一个同态. 类似的方法可以验证, Φ_{c_θ} 是绕轴 Ox_1 转角为 θ 的一个旋转. 现在对于任意矩阵 $A\in\mathrm{SO}(3)$ 有

$$A=B_\varphi C_\theta B_\psi=\Phi_{b_\varphi}\Phi_{c_\theta}\Phi_{b_\psi}=\Phi_{b_\varphi c_\theta b_\psi}=\Phi_{a(\varphi,\theta,\psi)}.$$

于是, 像 $\mathrm{Im}\Phi$ 包含整个群 SO(3), 即我们证得了

定理 1 在同态 $\Phi:g\mapsto\Phi_g$ 下, 群 SO(3) 是群 SU(2) 的同态像, 其核 $\mathrm{Ker}\Phi=\{\pm E\}$. SO(3) 中每个元素恰好与 SU(2) 中的两个酉算子 g 和 $-g$ 相对应.

4. 群 SO(3) 的几何表示 由定理 1 可以直接得到

推论 *群 SO(3) 拓扑等价 (同胚) 于三维射影实空间 $\mathbb{RP}^3$.*

事实上, 我们在第 2 目已经看到, SU(2) 的元素与四维实空间 $\mathbb{R}^4$ 中球面 S^3 上的点有一一对应. 线性算子 $\pm g \in \mathrm{SU}(2)$ 对应于 S^3 上的径对映点, 它们在同态 Φ 下粘合 (看作一样的). 于是得到了射影空间 $\mathbb{RP}^3$ 的一个模型. □

在线性代数和几何教程中 (见 [BA II], 第 5 章 §3), 射影空间 $\mathbb{RP}^n$ 被定义为经过坐标原点 O 的空间 $\mathbb{R}^{n+1}$ 中的直线的集合. 每个这样的直线恰好贯穿中心在原点的单位球, 交于两个径对映点. 直线通过这些点的一个表达式被唯一地复原. 这就是说, 空间 $\mathbb{RP}^n$ 可以定义为 $\mathbb{R}^{n+1}$ 中单位球关于球面 S^n 的径对映点的等价关系的商空间. $\mathbb{RP}^n$ 上的拓扑表述目前不列入我们的研究.

我们得到了相当意外的结果. 在球面 S^3 上和在射影空间 $\mathbb{RP}^3$ 上建立了群的结构: 在第一种情况下是 SU(2), 在第二种情况下, 是 SO(3). 在 S^2 上或在 $\mathbb{RP}^2$ 上构造连续群的任何尝试都以失败告终 (该结果与我们的主题无关).

根据定理 1 及其推论, SO(3) 是群 SU(2) 的二分之一. 由于存在 $\mathrm{SU}(2) \to \mathrm{SO}(3)$ 的满同态, 自然地产生是否存在 $\mathrm{SO}(3) \to \mathrm{SU}(2)$ 的同态的问题. 在第 3 章我们将看到这个问题的回答是否定的.

5. 四元数 如果在 $\mathbb{R}^4$ 上我们来理解特殊四维实空间, 它附有体的结构 —— 结合的, 哪怕是在 $\mathbb{R}$ 上带有除法 (所有非零元可逆) 的非交换代数, 那么 SU(2) 就变得更加直观. 我们现在所要说的著名的**四元数代数**, 是由哈密尔顿 (W. Hamilton, 1805—1865) 于 1848 年创立的, 为了表示对他的尊敬, 我们用符号 $\mathbb{H}$ 表示它. 按照习惯, 对于它的基元素用符号 **1** (单位元), **i** (虚数单位), **j** 和 **k** 表示. 因为在 $\mathbb{H}$ 中满足分配律, 所以乘法规则完全由下面 “乘法表” 所确定:

	1	**i**	**j**	**k**
1	**1**	**i**	**j**	**k**
i	**i**	**−1**	**k**	**−j**
j	**j**	**−k**	**−1**	**i**
k	**k**	**j**	**−i**	**−1**

从该表可以立即看出, $\mathbb{H}$ 是一个结合的 (但非交换的) 代数, 其中心 $Z(\mathbb{H}) = \mathbb{R}$, 且 **1** 是它的单位元. 代数 $\mathbb{H}$ 的每个元可以唯一地表示为下列形式

$$\mathbf{q} = \alpha + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k} := \alpha\mathbf{1} + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k} \tag{10}$$

其中 $\alpha, \beta, \gamma, \delta$ 为实系数, 于是

$$\mathbb{H} = \mathbb{R}\mathbf{1} + \mathbb{R}\mathbf{i} + \mathbb{R}\mathbf{j} + \mathbb{R}\mathbf{k}.$$

顺便指出, $\mathbb{H}$ 中的乘法是复数域 $\mathbb{C}$ 上乘法的直接延拓, 因为复数域恰好由那样的四元素 $\alpha+\beta\mathbf{i}$ 组成 ($\mathbf{1}$ 为实数, 而 $i=\sqrt{-1}$). 实际上, $\mathbb{H}$ 可以看作为复数域 $\mathbb{C}$ 上的二维代数. 事实上, 对于 $c, c' \in \mathbb{C}, \mathbf{q}, \mathbf{q}' \in \mathbb{H}$, 我们有

$$c(\mathbf{q}+\mathbf{q}')=c\mathbf{q}+c\mathbf{q}', \quad (c+c')\mathbf{q}=c\mathbf{q}+c'\mathbf{q}, \quad cc'(\mathbf{q})=c(c'\mathbf{q})=c'(c\mathbf{q}).$$

因为

$$\alpha\mathbf{1}+\beta\mathbf{i}+\gamma\mathbf{j}+\delta\mathbf{k}=(\alpha+\beta\sqrt{-1})\mathbf{1}+(\gamma+\delta\sqrt{-1})\mathbf{j},$$

所以 $\dim_{\mathbb{C}}\mathbb{H}=2$.

我们将在下面看到与 $\mathbb{C}$ 的类比. 四元数

$$\mathbf{q}^*=\alpha-\beta\mathbf{i}-\gamma\mathbf{j}-\delta\mathbf{k}$$

称为 $\mathbf{q}$ 的**共轭四元数**, 这类似于复数的共轭复数. 如果 $\mathbf{q}$ 是"纯四元数", 即 $\alpha=0$, 那么 $\mathbf{q}^*=-\mathbf{q}$. 通过上面的表算出并简化而得到的值

$$N(\mathbf{q}):=\mathbf{q}\cdot\mathbf{q}^*=\alpha^2+\beta^2+\gamma^2+\delta^2, \tag{11}$$

称为四元数 $\mathbf{q}$ 的**范数**. 显然, 如果 $\mathbf{q}\neq 0$, 则 $N(\mathbf{q})\neq 0$. 因此, 任意非零四元数可逆:

$$\mathbf{q}^{-1}=\frac{\mathbf{q}^*}{N(\mathbf{q})}, \quad \mathbf{q}\mathbf{q}^{-1}=\mathbf{1}=\mathbf{q}^{-1}\mathbf{q}. \tag{12}$$

于是, 集合 $\mathbb{H}^*:=\mathbb{H}\backslash\{0\}$ 是一个群 (称为**四元数代数乘法群**).

简单验证可以得到

$$(\mu_1\mathbf{q}_1+\mu_2\mathbf{q}_2)^*=\mu_1\mathbf{q}_1^*+\mu_2\mathbf{q}_2^*,$$
$$(\mathbf{q}_1\mathbf{q}_2)^*=\mathbf{q}_2^*\mathbf{q}_1^*$$
$$N(\mathbf{q}_1\mathbf{q}_2)=N(\mathbf{q}_1)N(\mathbf{q}_2).$$

这表明, 映射 $\mathbf{q}\to\mathbf{q}^*$ 是代数 $\mathbb{H}$ 的一个*反自同构* (改变因子的次序), 而映射 $\mathbf{q}\to N(\mathbf{q})$ 是乘法群 $\mathbb{H}^*$ 到 $\mathbb{R}^*$ 内的一个同态, 其同态核为

$$\mathrm{Sp}(1):=\mathrm{Ker}\,N=\{\mathbf{q}\in\mathbb{H}|N(\mathbf{q})=1\}. \tag{13}$$

群 Sp(1) 称为**辛群**, 它与线性辛群 $\mathrm{Sp}(2n,\mathfrak{K})$ 有直接的关系 (线性辛群在 [BA II] 中有扼要介绍), 但我们不在这里停顿.

由 (10), (11) 和 (13) 可以看出, 群 Sp(1) 拓扑等价于特殊四维空间 $\mathbb{H}$ 中的球面. 至于 SU(2) 的类似的性质, 我们在第 2 目已经见到. 将这种性质联系在一起不难. 考虑映射 $\Gamma:\mathbb{H}\to M_2(\mathbb{C})$, 它把形如 (10) 的每个四元数 $\mathbf{q}=c+\mathbf{j}c'$ 对应到复矩阵

$$\Gamma(\mathbf{q})=\begin{pmatrix}\alpha+\mathbf{i}\beta & \gamma+\mathbf{i}\delta\\ -(\gamma-\mathbf{i}\delta) & \alpha-\mathbf{i}\beta\end{pmatrix}=\begin{pmatrix}c & c'\\ -\overline{c'} & \overline{c}\end{pmatrix}. \tag{14}$$

显然,

$$\Gamma(\mu_1\mathbf{q}_1+\mu_2\mathbf{q}_2)=\mu_1\Gamma(\mathbf{q}_1)+\mu_2\Gamma(\mathbf{q}_2),$$
$$\Gamma(\mathbf{q}_1\mathbf{q}_2)=\Gamma(\mathbf{q}_1)\Gamma(\mathbf{q}_2),$$
$$\Gamma(\mathbf{1})=E.$$

就一般来说, 这是 $\mathbb{C}$ 上的一个**线性表示**, 该概念后面将会介绍. 顺便回想一下, 在 [BA I] 第 5 章, 最简单的代数变换将复数变为矩阵 $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M_2(\mathbb{R})$.

由 (14) 推得

$$\Gamma(\mathrm{Sp}(1))=\left\{\left(\begin{array}{cc} c & c' \\ -\overline{c'} & \bar{c} \end{array}\right)\middle|\, |c|^2+|c'|^2=1\right\}=\mathrm{SU}(2),$$

即 Γ 实现了群 SU(2) 与 Sp(1) 的同构. 为了寻找 $\mathrm{Sp}(1)\to\mathrm{SO}(3)$ 的满同态, 我们作下列映射. 将每个具有单位范数的四元数 $\mathbf{q}$ 对应一个映射 $\psi_{\mathbf{q}}:\mathbb{H}\to\mathbb{H}$,

$$\psi_{\mathbf{q}}(\mathbf{p})=\mathbf{q}\mathbf{p}\mathbf{q}^{-1}. \tag{15}$$

因为 $\mathbf{q}^{-1}=\mathbf{q}^*$ (见 (12)), 所以

$$\psi_{\mathbf{q}}(\mathbf{p}^*)=\mathbf{q}\mathbf{p}^*\mathbf{q}^{-1}=(\mathbf{q}^{-1})^*\mathbf{p}^*\mathbf{q}^*=(\psi_{\mathbf{q}}(\mathbf{p}))^*.$$

如果 $\mathbf{p}^*=-\mathbf{p}$ 为纯虚数, 那么 $(\psi_{\mathbf{q}}(\mathbf{p}))^*=\psi_{\mathbf{q}}(\mathbf{p}^*)=-\psi_{\mathbf{q}}(\mathbf{p})$. 于是纯四元数的子空间 $\mathbb{H}^-$ 对于 $\psi_{\mathbf{q}}$ 不变. 这样我们得到了线性算子

$$\psi_{\mathbf{q}}:\mathbb{H}^-\to\mathbb{H}^-.$$

由 (15) 可以直接推得, $\psi_{\mathbf{q}_1\mathbf{q}_2}=\psi_{\mathbf{q}_1}\psi_{\mathbf{q}_2}$, 也就是说, 群 Sp(1) 中的元可由三阶矩阵"表示":

$$\psi_{\mathbf{q}}(x_1\mathbf{i}+x_2\mathbf{j}+x_3\mathbf{k})=y_1\mathbf{i}+y_2\mathbf{j}+y_3\mathbf{k},\quad y_\mu=\sum_{\nu=1}^{3}a_{\mu\nu}x_\nu.$$

将三维欧氏空间 $\mathbb{R}^3$ 和纯四元数空间看作相同:

$$\mathbb{R}^3=\{\mathbf{p}\in\mathbb{H}^-\,|\,|\mathbf{p}|^2:=N(p)\}.$$

从这种长度平方 $|\mathbf{p}|^2$ 的定义, 有

$$|\psi_{\mathbf{q}}(\mathbf{p})|^2=N(\psi_{\mathbf{q}}(\mathbf{p}))=N(\mathbf{q})|\mathbf{p}|^2N(\mathbf{q}^{-1})=|\mathbf{p}|^2,$$

因为由条件 $N(\mathbf{q})=1$. 于是, $\psi_{\mathbf{q}}$ 是一个保持长度的线性算子, 且有同态 $\psi:\mathrm{Sp}(1)\to\mathrm{O}(3)$. 值得再次指出, $\psi_{\mathbf{q}}=\mathscr{E}$ 只有当 $\mathbf{q}=\pm 1$ 时成立, 因此 $\mathrm{Ker}\,\psi=\{\pm 1\}$.

现在回想一下 $\mathrm{Sp}(1)\sim S^3$. 因为任意点 $\mathbf{q}\in S^3$ 可以用光滑曲线 $\mathbf{r}(t)$ 使之与点 $\mathbf{1}$ 连接起来, 所以 $\Psi_{\mathbf{r}(t)}$ 是连接 $\psi_{\mathbf{q}}$ 与恒等算子 Ψ_1 的曲线. 行列式 det 是关于参数 t 的算子的连续函数, 且由于 $\det\Psi_{\mathbf{1}}=1$, 所以 $\det\Psi_{\mathbf{r}(t)}=1$. 特别地, $\det\Psi_{\mathbf{q}}=1$. 于是 $\Psi_{\mathrm{Sp}(1)}\subset\mathrm{SO}(3)$.

下面只需验证 Ψ 是一个满射. 为此我们让我们熟悉的矩阵 (1) 作为像.

$\mathbf{q}=\cos\dfrac{\theta}{2}\mathbf{1}+\sin\dfrac{\theta}{2}\mathbf{i}\Longrightarrow\psi_{\mathbf{q}}(\mathbf{i})=\mathbf{i}$, 即 $\mathbb{R}^3$ 中轴 $\mathbf{i}$ 在这个变换下是不变的. 因为

$$\psi_{\mathbf{q}}(\mathbf{j})\left(\cos\frac{\theta}{2}\mathbf{1}+\sin\frac{\theta}{2}\mathbf{i}\right)\mathbf{j}\left(\cos\frac{\theta}{2}\mathbf{1}-\sin\frac{\theta}{2}\mathbf{i}\right)=\cos\theta\mathbf{j}+\sin\theta\mathbf{k},$$
$$\psi_{\mathbf{q}}(\mathbf{k})=-\sin\theta\mathbf{j}+\cos\theta\mathbf{k}.$$

所以 $\psi_{\mathbf{q}}$ 具有矩阵 C_θ. 类似地, 如果 $\mathbf{q}=\cos\dfrac{\varphi}{2}\mathbf{1}+\sin\dfrac{\varphi}{2}\mathbf{k}$, 那么 $\psi_{\mathbf{q}}$ 具有绕 $\mathbf{k}$ 轴旋转的矩阵 B_φ.

于是, 下列定理正确.

定理 1′ *映射 Ψ (相应地 $\Psi\Gamma^{-1}$) 是群 $\mathrm{Sp}(1)$ (相应地 $\mathrm{SU}(2)$) 到群 $\mathrm{SO}(3)$ 的同态, 其同态核为 $\{\pm1\}$ (相应地 $\{\pm E\}$).*

习 题

1. 利用群 SU(2) 的几何描述, 证明

$$(0,1,0,0)*(0,0,1,0)=(0,0,0,1)\neq(0,0,1,0)*(0,1,0,0)$$

(S^3 上点的乘积). 而当点 $(0,1,0,0),(0,0,1,0)$ 看作 $\mathbb{RP}^3$ 上的点时, 相乘可交换.

2. 证明, 如果酉矩阵

$$K_1(t)=\begin{pmatrix}\cos\frac{t}{2} & i\sin\frac{t}{2}\\ i\sin\frac{t}{2} & \cos\frac{t}{2}\end{pmatrix},\quad K_2(t)=\begin{pmatrix}\cos\frac{t}{2} & -\sin\frac{t}{2}\\ \sin\frac{t}{2} & \cos\frac{t}{2}\end{pmatrix},\quad K_3(t)=\begin{pmatrix}e^{\frac{it}{2}} & 0\\ 0 & e^{\frac{-it}{2}}\end{pmatrix}$$

关于 t 求导数并随后令 $t=0$, 那么得到的矩阵

$$K_1=\frac{i}{2}\begin{pmatrix}0&1\\1&0\end{pmatrix}=\frac{i}{2}h_1,\quad K_2=\frac{i}{2}\begin{pmatrix}0&i\\-i&0\end{pmatrix}=\frac{i}{2}h_2,\quad K_3=\frac{i}{2}\begin{pmatrix}1&0\\0&-1\end{pmatrix}=\frac{i}{2}h_3$$

是迹为 0 的反埃尔米特矩阵空间 $(K^*=-K,\mathrm{tr}K=0)$ M_2^- 的基.

3. 四元数的单位 $\mathbf{i},\mathbf{j},\mathbf{k}$ 在 $\mathrm{Sp}(1)$ 中生成一个有趣的子群 —— 阶为 8 的四元数群 Q_8, 该群在各种问题中扮演着引人注目的角色. 试问矩阵

$$\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad\pm\begin{pmatrix}i&0\\0&-i\end{pmatrix},\quad\pm\begin{pmatrix}0&1\\-1&0\end{pmatrix},\quad\pm\begin{pmatrix}0&i\\i&0\end{pmatrix}$$

与四元数群 Q_8 有什么关系?

4. 能否在 $\mathbb{R}$ 上构造一个具有除法的三维结合代数 A, 它包含 $\mathbb{C}$ 作为子代数?

5. 很庆幸, 正是由于四元数的发现, 导致了四元数函数 (复变量函数的类似物) 学派的建立. 显然这方面还没有获得大量的成就, 但不可否认, 四元数与数学物理有着直接的关系. 通过在具有基 $\{\mathbf{i},\mathbf{j},\mathbf{k}\}$ 的三维泛函空间上引入微分算子

$$\nabla = \mathbf{i}\frac{\partial}{\partial x} + \mathbf{j}\frac{\partial}{\partial y} + \mathbf{k}\frac{\partial}{\partial z},$$

在某些程度上可以看出这一点. 下列关系是正确的:

$$\nabla t = \mathbf{i}\frac{\partial t}{\partial x} + \mathbf{j}\frac{\partial t}{\partial y} + \mathbf{k}\frac{\partial t}{\partial z},$$

它是数量 t 的斜率;

$$\nabla^2 t = -\Delta t = -\left(\frac{\partial^2 t}{\partial x^2} + \frac{\partial^2 t}{\partial y^2} + \frac{\partial^2 t}{\partial z^2}\right),$$

它是位势理论中的表达式;

$$\nabla(\underbrace{\mathbf{i}u + \mathbf{j}v + \mathbf{k}w}_{\text{场}}) = -\underbrace{\left(\frac{\partial u}{\partial x} + \frac{\partial v}{\partial y} + \frac{\partial w}{\partial z}\right)}_{\text{场的散度}} +$$
$$+\underbrace{\mathbf{i}\left(\frac{\partial w}{\partial y} - \frac{\partial v}{\partial z}\right) + \mathbf{j}\left(\frac{\partial u}{\partial z} - \frac{\partial w}{\partial x}\right) + \mathbf{k}\left(\frac{\partial v}{\partial x} - \frac{\partial u}{\partial y}\right)}_{\text{场的旋度}}.$$

所有这些计算都依靠了四元数代数中的乘法.

§2 子群的陪集

1. 初等性质　假设 G, G', 是两个任意群, 它们分别具有单位元 e, e'. 由定义, 一个同态 $f: G \to G'$, 以及由我们在 [BA I, BA II] 中的大量的例子所见到的, $\operatorname{Ker} f$ 为 G 的一个子群, 而且 $x(\operatorname{Ker} f) = (\operatorname{Ker} f)x, \forall x \in G$.

定义　*群 G 的一个子群 K 称为在 G 中***正规的**, *如果*

$$xKx^{-1} = K, \quad \forall x \in G.$$

于是, 同态核总是 G 的一个正规子群. 这个事实的重要性稍后我们进行适当的评价. 我们指出, 并不是任意子群都在 G 中正规. 例如, 在 S_3 中, 循环子群 $\langle(123)\rangle = A_3$ 正规, 但 $\langle(12)\rangle = \{e, (12)\}$ 不正规.

我们现在将注意力转到这样的情形, 群 G 中元素集合

$$a\operatorname{Ker} f = \{ab | b \in \operatorname{Ker} f\}, \quad a \in G,$$

映射到 G' 中唯一的元 $f(a)$: $f(ab) = f(a)f(b) = f(a)e' = f(a)$. 同样, 如果 $f(g) = f(a)$, 那么 $f(a^{-1}g) = f(a^{-1})f(g) = f(a)^{-1}f(g) = e'$, 由此得到 $a^{-1}g = b \in \operatorname{Ker} f$, 从

而 $g = ab \in a\mathrm{Ker}\, f$. 这表明, 形如 $a\mathrm{Ker}\, f$ 的子集构成 G 的一个分类. 这种分类一般情况下不依赖于同态.

定义 设 H 是群 G 的一个子群. 子集 $gH = \{gh | g$ 是 G 中的一个固定元, h 跑遍 H 的所有元 $\}$ 称为群 G 关于子群 H 的一个**左陪集**. 元素 g 称为陪集 gH 的一个**代表元**.

类似地, 我们可以定义**右陪集**. 有时我们的左陪集也被称为右陪集, 而右陪集称为左陪集, 关键是要遵循某一习惯. 如果 $H = \mathrm{Ker}\, f$ 为同态核, 那么 $gH = Hg$, 因为 H 是 G 的正规子群. 我们指出, 子群 $H = He = eH$ 本身就是一个陪集. 其它任何陪集都不是子群. 事实上, 如果 gH 是子群, 则 $e \in gH$, 从而 $e = gh, g = h^{-1}$, 于是 $gH = h^{-1}H = H$.

定理 1 *群 G 关于子群 H 的两个左陪集要么相等要么没有公共元. G 关于 H 的左陪集分解决定了群 G 的元素之间的一个等价关系.*

证明 假如陪集 g_1H 和 g_2H 有公共元 $a = g_1h_1 = g_2h_2$. 那么 $g_2 = g_1h_1h_2^{-1}$, 从而 g_2H 类的任意元 g_2h 有形式 $g_1h_1h_2^{-1}h = g_1h'$, 这里 $h' = h_1h_2^{-1}h \in H$. 于是 $g_2H \subset g_1H$. 类似地, g_1H 的任意元含于 g_2H, 因此 $g_1H = g_2H$.

因为任意给定一个元 $g \in G$, 有 $g \in gH$, 所以上述论断表明 G 可以分解为子群 H 的两两不相交的左陪集的并:

$$G = \bigcup_i g_iH.$$

按照在 [BA I] 第 1 章 §6 中所述的一般原理, 这个分解在 G 上诱导一个等价关系, 其定义形式为:

$$a \sim b \Longleftrightarrow a^{-1}b \in H.$$

这个关系的自反性、对称性和传递性可以直接验证: $a \sim a$, 因为 $a^{-1}a = e \in H$; $a \sim b \Longleftrightarrow a^{-1}b = h \Longleftrightarrow b^{-1}a = h^{-1} \in H \Longleftrightarrow b \sim a$; $a \sim b, b \sim c \Longrightarrow b^{-1}a = h_1, c^{-1}b = h_2 \Longrightarrow c^{-1}a = c^{-1}bh_1 = h_2h_1 \in H \Longrightarrow a \sim c$. □

对于右陪集有类似的命题.

对置换群可利用自然方式产生陪集分解. 譬如, 令 $G = S_n$ 为作用在集合 $\Omega = \{1, 2, \cdots, n\}$ 上的对称群. 如果我们将满足 $\pi(n) = n$ 的 S_n 中的元素 π 的全体记为 H, 则不难验证 H 是 S_n 的一个子群, 并可将它看作与 S_{n-1} 相同. 令 $\tau_0 = e, \tau_i = (i, n)$ 为 n 与 $i (i = 1, 2, \cdots, n-1)$ 的对换. 则显然

$$S_n = \bigcup_{k=0}^{n-1} \tau_k S_{n-1}.$$

我们看 S_3 关于子群 $\langle(12)\rangle = S_2$ 的左陪集和右陪集分解:

$$S_3 = \{e,(12)\} \cup \{(13),(123)\} \cup \{(23),(132)\},$$
$$S_3 = \{e,(12)\} \cup \{(13),(132)\} \cup \{(23),(123)\}.$$

我们看到, 左陪集 gS_2 的集合不等于右陪集 S_2g' 的集合, 然而在集合 $\{gH\}$ 和 $\{Hg'\}$ 之间总有一个一一对应, 且

$$x = gh \in gH \Longleftrightarrow x^{-1} = h^{-1}g^{-1} \in Hg^{-1}.$$

事实上, 如果, 例如, $h_1g_1^{-1} = h_2g_2^{-1}$, 那么 $g_1 = g_2h_2^{-1}h_1$; 从而 $g_1H = g_2H$. 于是, *如果 $\{e,x,y,z,\cdots\}$ 是左陪集 (相应地右陪集) 的代表元之集, 那么 $\{e,x^{-1},y^{-1},z^{-1},\cdots\}$ 就是右陪集 (相应地左陪集) 的代表元之集*. 于是这两个集合的势相等. □

群 G 关于子群 H 的所有左陪集的集合我们用 G/H 表示 (如果同时出现右陪集的集合 $(G/H)_r$, 则左陪集可用 $(G/H)_l$ 表示, 以示区分). 对于这个集合 G/H 的势 $\mathrm{Card}\, G/H$, 称为 "*子集 H 在 G 中的指数*", 并利用专门的符号 $(G:H)$ 表示, 它与群 G 的阶 $|G|$ 的表示 $(G:e)$ 相一致, ($(G:e)$ 为 G 关于单位子群的陪集个数). 因为映射 $H \to gH$ 为彼此单值对应 (参见凯莱定理的证明及其映射 L_g), 所以 $\mathrm{Card}\, gH = (H:e)$. 因此我们得到公式

$$(G:e) = (G:H)(H:e).$$

由此得到下列经典的

定理 2 (拉格朗日 (Lagrange)) *有限群 G 的阶被它的每个子群的阶整除.*

推论 *群的任一元的阶整除群的阶. 素数 p 阶群总为循环群且精确到同构是唯一的.*

事实上, 任意元 $g \in G$ 的阶等于由它生成的循环子群 $\langle g\rangle$ 的阶 ([BA I], 第 4 章 §2 定理 2). 其次, 如果 $|G| = p$ 为一个素数, 而 H 为 G 的非单位子群, 则 $p \mid |H|$, 于是 $|H| = p$, 从而 $H = G$. 可见 G 等于由它的任意非单位元 g 生成的循环子群. 所有相同阶的循环群互相同构 ([BA I], 第 4 章 §2 定理 3), 这回答了唯一性的问题. □

由拉格朗日定理产生了一个 "诱惑": 对于群 G 的阶为 n 的每个因子 m, 去寻找 G 中的 m 阶子群. 但这方面总的讲没有基本原理. 愿意者可以去检验 (留作练习), 在阶为 12 的交错群 A_4 中没有 6 阶子群. 然而, 正如我们现在所看到的, 在某些群中 "拉格朗日定理的逆" 是正确的.

2. 循环群的结构 由 [BA I] 中我们已经知道, 所有同阶的循环群是同构的, 而在任意群中元素的阶等于由该元素生成的循环子群的阶. 实际上有下面的

定理 3 循环群的任一子群还是一个循环群. 无限循环群 $(\mathbb{Z},+)$ 的子群只限于 (无限) 子群 $(m\mathbb{Z},+), m\in\mathbb{N}$, 而阶为 q 的循环群的子群与数 q 的因子 d 一一对应.

证明 我们不妨换个方式来看运算为加法的任意循环群 $A=\langle a\rangle$. 该群的每个元素有形式 ka, 这里 $k\in\mathbb{Z}$ 或 $k=0,1,\cdots,q-1$, 如果 A 是 q 阶有限群. 令 B 为 A 的非零子群, 如果 $ka\in B$ 对于某个 $k\neq 0$, 则 $-ka\in B$. 在所有带有正数 k 的元素 $ka\in B$ 中选择一个元素 ma, 其 m 为最小数.

对任意 $k>0$, 设 $k=lm+r, 0\leqslant r<m$, 由 $ka\in B$, 我们有 $ra=ka-l(ma)\in B$, 于是 $r=0$. 这表明 $B=\langle ma\rangle$ 为循环群.

所有无限循环群同构于 $(\mathbb{Z},+)$. 于是由上面讨论知 $(\mathbb{Z},+)$ 的任意子群可以由一个自然数 m 所确定且有形式

$$m\mathbb{Z}=\langle m\cdot 1\rangle=\{0,\pm m,\pm 2m,\cdots\}.$$

显然它的所有子群是无限群.①

现在令 $\langle a\rangle=\{0,a,\cdots,(q-1)a\}, qa=0$. 我们知道, $B=\{0,ma,2ma,\cdots\}$, 这里 $m\in\mathbb{N}$, 且 $sa\in B, s\in\mathbb{N}\Longrightarrow s=mt$. 我们证明 m 整除 q. 事实上, 令 $q=dm+r, 0\leqslant r<m$. 则

$$0=qa=d(ma)+ra,$$

由此得到 $ra=-d(ma)\in B$. 由 m 的极小性推得 $r=0$. 于是 $q=dm$. 因而

$$B=\{0,ma,2ma,\cdots,(d-1)ma\}=mA.$$

它是 A 的阶为 d 的子群. 当 m 跑遍数 q 的所有正因子, 那么 d 也一样, 我们得到每个 d 阶子群, 这里 d 整除 q. □

推论 在阶为 q 的循环群 $\langle a\rangle$ 中, 阶为 d 的子群 (这里 $d|q$) 等于这样一些元素 $b\in\langle a\rangle$ 的集合, 它满足 $db=0$.

证明 如果 $dm=q$, 那么 $b\in B=mA$, 从而 $db=0$. 反之, 假设 $b=la\in\langle a\rangle$ 满足 $db=0$. 则由 $dla=0$ 推得 $dl=qk=dmk$, 于是 $l=mk$ 且 $b=la=k(ma)\in mA$. □

习 题

1. 证明: 在任一群中, 指数为 2 的子群一定是正规的.
2. 利用习题 1 试证, 就同构而言, S_3 是唯一的 6 阶非交换群.

①这是指非平凡子群 —— 译者注.

§3 群在集合上的作用

1. $G \to S(\Omega)$ 的同态 在 [BA I] 第 4 章, 我们通过变换群, 即群 $S(\Omega)$ 的子群开始介绍群的理论, 这里 $S(\Omega)$ 为集合 Ω 到自身上的所有一一映射构成的群. 这种方法符合群论发展的历史, 而且与变换群在其它数学领域的重要性相应. 所谓抽象群论是更晚期的产物 (20 世纪上半叶), 早已远离了变换群, 但它的许多概念仍带有旧时的印迹. 也就是说, 这些概念的来源经常建立在给定群 G 到 $S(\Omega)$ 的实现的思想基础上, 这里 Ω 是以适当方式选定的某一集合. 利用任一同态 $\Phi: G \to S(\Omega)$ 使 G 到 $S(\Omega)$ 中. 如果 Φ_g 是 $S(\Omega)$ 中对应于元素 $g \in G$ 的一个变换, 则 $\Phi_e = e_\Omega$ 是 $\Omega \to \Omega$ 的恒等变换, 且 $\Phi_{gh} = \Phi_g \circ \Phi_h, g, h \in G$. 点 $x \in \Omega$ 在变换 Φ_g 下的像 $\Phi_g(x)$ 常常用一个符号 gx 表示, 这也可以说成是笛卡儿积 $G \times \Omega$ 到 Ω 的一个映射 $(g, x) \mapsto gx$. 为了不与 G 中的乘法造成混乱, 更规范地可以写成 $g \circ x$ 或 $g * x$, 但一般地, 这没有必要. 我们将上面变换 Φ_g 的性质写成下列形式:

i) $ex = x, x \in \Omega$;

ii) $(gh)x = g(hx), g, h \in G$.

每当笛卡儿积 $G \times \Omega$ 到 Ω 的映射 $(g, x) \to gx$ 满足性质 i) 和 ii) 时, 我们就称群 G (从左) *作用*在集合 Ω 上, 而称 Ω 是一个 G–集. 另一方面, 如果有 G–集 Ω, 我们借助于公式

$$\Phi_g(x) = gx, \quad x \in \Omega$$

对每个 $g \in G$, 定义一个映射 $\Phi_g : \Omega \to \Omega$, 且由 i), ii) 有 $\Phi : g \mapsto \Phi_g$ 将得到一个 G 到 $S(\Omega)$ 内的一个同态. 我们也称 (特别是当 $|\Omega| < \infty$) 群 G 在 Ω 上的作用对应*群到置换群的一个表示*(Φ, Ω), 核 $\mathrm{Ker}\Phi$ 称为**群作用的核**. 如果 Φ 是一个单一同态 (即: 如果 $gx = x, \forall x \in \Omega$, 则 $g = e$), 那么称群 G **忠实地**作用在集合 Ω 上.

注 群 G 到 Ω 上的每个作用由规则 $g(x_1, \cdots, x_k) = (gx_1, \cdots, gx_k)$ 诱导一个 G 到 $\Omega^k = \Omega \times \cdots \times \Omega$ 上的作用, 此外, 存在 G 到所有子集的集合 $\mathcal{P}(\Omega)$ 上的作用 (参见 [BA I], 第 1 章 §5 习题 4). 我们规定 $g\varnothing = \varnothing$, 而如果 T 是 Ω 的非空子集, 则 $gT = \{gt | t \in T\}$. 性质 i), ii) 可直接验证. 易见, T 和 gT 有相同的势, 于是 G 诱导一个在相同势的子集上的作用.

2. 轨道和点的稳定子群. 两个点 $x, x' \in \Omega$ 称为关于群 G 在 Ω 上的作用是等价的, 如果存在某一个元 $g \in G$ 使得 $x' = gx$. 该关系的反身性、对称性和传递性很容易由性质 i), ii) 得到 (参见第 1 目), 这表明我们涉及的是真的等价关系, 从而把 Ω 分成两两不相交的等价类. 这种等价类通常称为 G–轨道. 包含元素 $x_0 \in \Omega$ 的轨道自然地记为 $G(x_0)$, 于是 $G(x_0) = \{gx_0 | g \in G\}$. 但是, 也利用其它符号, 以强调 G 在 Ω 上的这样或那样的作用特征. 轨道的概念来自于几何. 例如, 如果 $G = \mathrm{SO}(2)$ 为平面上绕原点 O 的旋转群, 那么点 P 的轨道就是经过 P 点的中心为 O 的圆 (圆周).

而集合 $\Omega = \mathbb{R}^2$ 是所有同心圆的并, 这些同心圆包括零半径的圆 (即点 O). 对于我们来说, 轨道的概念也不是新的. 我们在 [BA I] 第 4 章关于分解置换 $\pi \in S_n$ 为不相交循环置换时就已用到轨道的概念. 取循环群 $\langle \pi \rangle$ 作为 G.

令 x_0 为 Ω 中的一个固定点. 我们来看集合

$$\mathrm{St}(x_0) = \{g \in G | gx_0 = x_0\} \subset G.$$

因为 $ex_0 = x_0$, 且由 $g, h \in \mathrm{St}(x_0) \Longrightarrow gh^{-1} \in \mathrm{St}(x_0)$, 所以 $\mathrm{St}(x_0)$ 是群 G 的一个子群, 它称为点 $x_0 \in \Omega$ 的稳定子群 (或中心化子), 并常被表示为 G_{x_0}. 我们来看上面的群 $\mathrm{SO}(2)$ 在 $\mathbb{R}^2$ 上的作用, 则我们有 $\mathrm{St}(0) = \mathrm{SO}(2)$, 而且如果点 $P \neq O$, 则 $\mathrm{St}(P) = e$. 在一般情况下.

$$gx_0 = g'x_0 \Longleftrightarrow g^{-1}g' \in \mathrm{St}(x_0) \Longleftrightarrow g' \in g\mathrm{St}(x_0).$$

可见, 群 G 中稳定子群 $\mathrm{St}(x_0)$ 的左陪集 $g\mathrm{St}(x_0)$ 与轨道 $G(x_0)$ 的点一一对应. 特别地,

$$\mathrm{Card}\, G(x_0) = \mathrm{Card}(G/\mathrm{St}(x_0)) = (G : \mathrm{St}(x_0)). \tag{1}$$

这里 $G/\mathrm{St}(x_0)$ 是 G 关于 $\mathrm{St}(x_0)$ 的商群, 而 $(G : \mathrm{St}(x_0))$ 是子群 $\mathrm{St}(x_0)$ 在 G 中的指数. 基数 $\mathrm{Card}G(x_0)$ 常称为含点 x_0 的 G–轨道的长. 由 (1) 和拉格朗日定理知, 有限群 G 的任一轨道长是群 G 阶的因子.

我们注意另一情形: 等式右边的点 x_0 也可以用任一点 $x'_0 \in G(x_0)$ 来代替. 事实上

$$\mathrm{Card}\, G(x_0) = \mathrm{Card}\, G(x'_0) = (G : \mathrm{St}(x'_0)).$$

关于稳定子群的更有力的断言如下. 令 $x'_0 = gx_0$. 则

$$\mathrm{St}(x'_0)gx_0 = \mathrm{St}(x'_0)x'_0 = x'_0 = gx_0,$$

从而 $g^{-1}\mathrm{St}(x'_0)gx_0 = x_0$, 即

$$g^{-1}\mathrm{St}(x'_0)g \subset \mathrm{St}(x_0).$$

类似地, 因为

$$\mathrm{St}(x_0)g^{-1}x'_0 = \mathrm{St}(x_0)x_0 = x_0 = g^{-1}x'_0,$$

我们有

$$g\mathrm{St}(x_0)g^{-1} \subset \mathrm{St}(x'_0).$$

于是, 有等式

$$\mathrm{St}(x'_0) = g\mathrm{St}(x_0)g^{-1} = \{ghg^{-1} | h \in \mathrm{St}(x_0)\}.$$

在下面将看到的例 1 中, 我们把两个子群 $H, H' \subseteq G$ 称为共轭的, 如果 $H' = gHg'$ 对某个 $g \in G$ 成立. 我们将上面得到的结果准确地表达为下列定理的形式.

定理 1　设群 G 作用在集合 Ω 上. 如果两个点 $x_0, x_0' \in \Omega$ 位于同一个轨道, 那么它们的稳定子群共轭:

$$x_0' = gx_0 \Longrightarrow \mathrm{St}(x_0') = g\mathrm{St}(x_0)g^{-1}.$$

如果 G 还是有限群且

$$\Omega = \Omega_1 \cup \Omega_2 \cup \cdots \cup \Omega_r$$

为 Ω 的以 $x_1, x_2, \cdots, x_r$ 为代表元的有限多个轨道的分解, 则

$$|\Omega| = \sum_{i=1}^{r} (G : \mathrm{St}(x_i)). \tag{2}$$

公式 (2) 是许多使用 "轨道方法" 到有限群的基础.

3. 群作用在集合上的例子　我们仅选取一些本身与群论有关的例子.

例 1 (共轭作用)　在 $\Omega = G$ 上利用下列公式定义任意元 $g \in G$ 的作用

$$x \mapsto I_g(x) = gxg^{-1}, \quad \forall x \in G.$$

当然也可以采用记号 $g \circ x = gxg^{-1}$, 但是我们更喜欢使用在 [BA I], 第 4 章 §2 第 4 目中对于 $g \in G$ 使用过的内自同构记号 I_g.

元素 g 的作用, 与 $\mathrm{Inn}\, G$ 的作用相同, 称为**共轭** (或**变换**). 它的核是群 G 的中心:

$$Z(G) = \{z \in G | I_g(z) = z, \forall g \in G\} = \{z \in G | zg = gz, \forall g \in G\}.$$

元素 $x \in G = \Omega$ 的轨道, 记为 x^G, 称为**共轭元素类**, 或简称为包含 x 的**共轭类**. 如果 $a, b \in x^G$, 那么有时也记为 $a \overset{G}{\sim} b$. 此时稳定子群 $\mathrm{St}(x)$ 称为元素 x 的**中心化子**, 并记为 $C(x)$ (或 $C_G(x)$ 若需要标出群 G).

共轭作用, 按照第 1 目后面的注, 转到群 G 的子集和子群. 两个子集 $H, T \subset G$ 共轭, 如果 $T = gHg^{-1}$, 对于某个 $g \in G$ 成立.

设 H 是 G 的一个子群. 通常称

$$N(H) := N_G(H) := \mathrm{St}(H) = \{g \in G | gHg^{-1} = H\}$$

为子群 H 在 G 中的**正规化子**. 特别地, 称 $H \lhd G$ (H 为 G 的正规子群), 如果 $N(H) = G$. 该定义与 §2 第 1 目的定义一致. 按照等式 (1), 轨道 H^G 的长 (即与 H 互相共轭的子群的个数) 等于正规化子 $N(H)$ 在 G 中的指数.

下面假设 G 是一个有限群, $x_1^G, x_2^G, \cdots, x_r^G$ 为它的共轭元素类, 并且它们中前 q 个共轭元素类只含一个元素:

$$x_i^G = \{x_i\}, \quad i = 1, \cdots, q (x_1 = e).$$

那么 $Z(G)=\{x_1,x_2,\cdots,x_q\}$, 而根据 (1) 和 (2) 有

$$|x_i^G|=(G:C_G(x_i))\quad i=1,\cdots,q,q+1,\cdots, \tag{1'}$$

$$|G|=|Z(G)|+\sum_{i=q+1}^{r}(G:C_G(x_i)). \tag{2'}$$

令 $G=S_3$, 则 $r=3,q=1$ (即 $Z(S_3)=e$) 且

$$S_3=\{e\}\cup\{(12),(13),(23)\}\cup\{(123),(132)\}$$

为 S_3 的共轭元素类分解. 正如 (1′) 所描述的, 这些类的长 (轨道长) 整除 $|S_3|=6$.

由 (2′) 立即得到下列有趣的结果.

定理 2 对任意有限 p–群 G (其阶 $p^n>1,p$ 是一个素数), 它的中心 $Z(G)\neq e$.

证明 如果 G 是交换群, 则 $G=Z(G)$, 于是结论成立. 假设 G 非交换, 即 $r>q$, 则当 $i>q$ 时, $(G:C(x_i))=p^{n_i},n_i\geqslant 1$ 且由 (2) 有

$$p^n=|Z(G)|+\sum_{i=q+1}^{r}p^{n_i},$$

于是显然有 $|Z(G)|$ 被 p 整除. □

非交换 p-群的存在性容易验证. 我们只要来看有限 p 元域上的三角形矩阵群

$$P=\left\{\begin{pmatrix}1&a&c\\0&1&b\\0&0&1\end{pmatrix}\middle|\, a,b,c\in Z_p\right\}.$$

例 2 (平移) 我们在证明凯莱定理 ([BA I], 第 4 章 § 2) 时所用的由公式 $L_a(g)=ag$ 给出的映射 $L_a:G\to G$, 通常称为用 a 的**左平移**. 因为 $eg=g$ 且 $(ab)g=a(bg)$, 所以左平移给出了 G 到自身上的作用, 该作用诱导群 G 在子集合上的作用. 譬如, 假设 H 是一个子群, G/H 为左陪集 $gH,g\in G$, 的集合.

显然, 映射

$$(x,gH)\mapsto x(gH)=(xg)H$$

定义了一个群 G 在 G/H 上的作用 L^H. 该作用的核 $\operatorname{Ker}L^H$ 是集合

$$\{x\in G|L_x^H(gH)=gH,\forall g\in G\}=\{x\in G|xgH=gH,\quad\forall g\in G\}.$$

换句话说, $x\in\operatorname{Ker}L^H\iff g^{-1}xg\in H,\forall g\in G$, 或等价地说 $x\in gHg^{-1},\forall g\in G$. 因此,

$$\operatorname{Ker}L^H=\bigcap_{g\in G}gHg^{-1}$$

是包含在 H 中的群 G 的最大正规子群. G 在 G/H 上作用的忠实性等价于说没有子群 $K \subset H$ 满足 $K \neq e$ 且 K 在 G 中正规.

这种用 L_x^H 在 G 关于 H 的陪集上的置换表示 $(L^H, G/H)$ 可用于在 G 中指数为 n 的任意子群. 这个表示 (可能, 不精确) 比借助于凯莱定理的应用所得到的要方便得多.

例 3 (可迁群) 作用在集合 $\Omega = \{1, 2, \cdots, n\}$ 上的置换群 $G \subset S_n$ 称为**可迁的**, 如果某个 (从而任意) 点 $i \in \Omega$ 的轨道 G_i 等于 Ω. 换句话说, 作用 $G \times \Omega \to \Omega$ 在 Ω 上可迁, 如果对任意两点 $i, j \in \Omega$, 至少存在一个元 $g \in G$ 使 $g(i) = j$.

令 $\Omega^{[k]}$ 为 Ω 中有序 k–元子集的全体. 作用在 Ω 上的群 G 在 $\Omega^{[k]}$ 上诱导一个作用; 如果它在 $\Omega^{[k]}$ 上可迁的, 则称 G 为 Ω 上 k–可迁. 譬如, 对称群 S_n 在 Ω 上是 n–可迁的, 而交错群 A_n 是 $(n-2)$–可迁的.

任意群 G 在 G 关于 H 的左陪集集合 G/H 上是可迁的 (参见例 2). 事实上, 如果 g_iH, g_jH 是两个左陪集, 那么 $g_jg_i^{-1}(g_iH) = g_jH$. 更奇怪的是, 用直接方法得到的关于给定指数 n 的群的 k–可迁信息 (在 $k > 5$ 时) 是很困难的. 走了很多弯路, 直到 20 世纪 80 年代初才证明了若当猜想: 所有这样的群只有两个: S_n 和 A_n.

我们收集在后面用得着的关于可迁群的所得的一些有趣的结果. 设 G 为 Ω 上的可迁群. 点 $i \in \Omega$ 的稳定子群 $\mathrm{St}(i)$ 用符号 G_i 表示. 我们已经知道 (参见定理 1), 如果 $i = g_i(1)$, 则 $G_i = g_iG_1g_i^{-1}, i = 1, 2, \cdots, n (g_1 = e)$. 此外, 元素 g_i 可以选为 G 关于 G_1 的左陪集的代表元:

$$G = G_1 \cup g_1G_1 \cup \cdots \cup g_nG_1. \tag{3}$$

特别地, 由轨道长的一般结果 (见第 2 目) 知 $|G| = n|G_1|$.

定理 3 设 G 是 Ω 上的一个可迁群, 且对任意 $g \in G$, 令 $N(g)$ 为在 g 作用下保持不变的 Ω 中点的个数. 那么

i) $\sum_{g \in G} N(g) = |G|$ (用 $|G|$ 除等式 i) 两边, 得到 "平均" 每个元保持一个点不动);

ii) 如果 G 是 2–可迁群, 那么 $\sum_{g \in G} N(g)^2 = 2|G|$.

证明 i) 我们有

$$\sum_{g \in G} N(g) = \sum_{j=1}^{n} \Gamma(j),$$

其中 $\Gamma(j)$ 是保持 j 不变的 G 中元素的个数. 换句话说, $\Gamma(j) = |G_j|$. 但是, 由可迁性,

$$|G_j| = |g_jG_1g_j^{-1}| = |G_1|,$$

这里 g_j 取自分解 (3). 于是

$$\sum_{g\in G} N(g)=\sum_{j=1}^{n}|G_j|=\sum_{j=1}^{n}|G_1|=n|G_1|=|G|.$$

ii) 2–可迁的条件意味着, 在集合 $\Omega_1=\Omega\backslash\{1\}$ 上的稳定子群 G_1 为可迁作用, 即 $\{1\}$ 和 Ω_1 为 G_1–轨道. 令 $N'(x)$ 为在 $x\in G$ 作用下不变的 Ω_1 中点的个数. 将 i) 用于 (G_1,Ω_1), 有

$$\sum_{x\in G_1} N'(x)=|G_1|.$$

因为对 $x\in G_1, N(x)=1+N'(x)$ (添加点 1). 所以有

$$\sum_{x\in G_1} N(x)=2|G_1|.$$

对于所有其它的 G_j, 同样有

$$\sum_{x\in G_j} N(x)=2|G_j|=2|G_1|.$$

对 j 取和, 我们得到

$$\sum_{j=1}^{n}\sum_{x\in G_j} N(x)=2n|G_1|=2|G|.$$

左边 $N(x)$ 被认为是分别对于包含 x 的每个子群 G_j 中的一个元. 但 x 仅仅保持 $N(x)$ 中的点不变, 所以左边包含的子集 G_j 的个数与 $N(x)$ 的大小一样. 于是每个 x 引起的总项数为 $N(x)^2$. 另一方面, 任意一个不包含在并 $\bigcup_j G_j$ 的 $y\in G$, 它变动所有元, 于是 $N(y)=0$. 因此, 我们可以写出下列等式

$$\sum_{g\in G} N(g)^2=\sum_{j=1}^{n}\sum_{x\in G_j} N(x)=2|G|. \qquad \square$$

4. 齐次空间 对于几何来说特别有趣的是 Ω 为拓扑空间 (譬如直线 $\mathbb{R}$ 或球面 S^2), 而 G 称为连续 (或拓扑) 群, 其作用 $(g,x)=gx$ 服从于合理的要求:

iii) $f(x)=gx$ 是两个变量 g 和 x 的连续函数.

作用在 Ω 上并满足前面性质 i), ii) 及现在的 iii) 的群 G 称为空间 Ω 的**运动群**. 在这种情况下, 也许作用保留某种 Ω 上的度量. 空间 Ω 称为**齐次的**, 如果 G 作用在 Ω 上可迁 (见例 3), 即 Ω 中所有点位于同一个 G–轨道.

由 1–2 段的一般观点, 显然在齐次空间 Ω 的点和 G 关于一个稳定子群的陪集之间有一一对应, 在这种情况下, 空间 Ω 的作用 $g\in G$ 对应一个集合 G/H 上的映射 $g'H\mapsto gg'H$.

我们从新的角度来看我们在 §1 中已熟悉的群 SO(3). 群 SO(3) 可以想象成单位半径的二维球面 S^2 上的作用. 显然, 任意一对点 $P, Q \in S^2$, 有某个作用 (旋转) 将 P 变到 Q, 即 S^2 是一个具有群 SO(3) 作用的齐次空间. 任意点 $P \in S^2$ 的稳定子群 $\mathrm{St}(P)$ 保持经过点 P 和球面的中心的整个轴不变. 因此 $\mathrm{St}(P) \cong \mathrm{SO}(2)$ 为垂直于直线 OP 的平面旋转群. 因为群 SO(2) 的元素可以看作与以单位半径为圆周 S^1 的点相同, 所以群 SO(3) 可以看作为一个大馅饼, 它的每一层是用二维球面 $\mathrm{SO}(3)/S^1 \approx S^2$ 的点编号的一个单位圆. 在这种情况下, 称之为具有基 S^2 和层 $p^{-1}(P) \approx S^1, P \in S^2$, 的分层 (投射 $p : \mathrm{SO}(3) \to S^2$). 所有这些概念的准确涵义在几何和拓扑学教程中已解释清楚了, 因此我们不再赘述.

习　题

1. 设 Φ 和 Φ' 分别为群到 $S(\Omega)$ 和 $S(\Omega')$ 的同态. 那么它们所确定的 Ω 上和 Ω' 上的作用称为**等价的**, 如果存在一个双射 $\sigma : \Omega \to \Omega'$, 使下图

$$\begin{array}{ccc} \Omega & \xrightarrow{\sigma} & \Omega' \\ {\scriptstyle\Phi_g}\downarrow & & \downarrow{\scriptstyle\Phi'_g} \\ \Omega & \xrightarrow{\sigma} & \Omega' \end{array}$$

对所有 $g \in G$ 是交换的. 于是 $\Phi'_g = \sigma\Phi_g\sigma^{-1}$. 证明, 群 G 的每个可迁作用等价于 G 关于某个子群 H 的左陪集上的作用.

2. 利用定理 2 证明, 所有阶为 p^2 的群 (这里 p 为一个素数) 是交换群.

3. 证明, 在例 1 末尾的群 P 的中心为

$$Z(P) = \left\{ \left. \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right| c \in Z_p \right\}.$$

找出群 P 的共轭类.

4. 令 n 为一个自然数. 我们将它写为和的形式 $n = n_1 + n_2 + \cdots + n_m$, 其中 $n_1 \geqslant n_2 \geqslant \cdots \geqslant n_m \geqslant 1$. 所有这样的具有 $m = 1, 2, \cdots$ 个分解的个数用 $p(n)$ 来表示. 于是 $p(3) = 3, p(4) = 5$, 等等. 每个置换 $\pi \in S_n$ 分解为无关的循环置换的乘积 (参看 [BA I], 第 1 章 §8) 的表达式 $\pi = \pi_1\pi_2\cdots\pi_m$ 唯一地确定数 n 的一个分解. 证明, 解 S_n 的共轭类与数 n 的分解有一个一一对应.

5. 设置换 $\pi \in S_n$ 分解为 r 个长为 1 的循环置换, S 个长为 2 的循环置换, t 个长为 3 的循环置换, ……, 的乘积, 那么 $n = r + 2s + 3t + \cdots$. 证明, S_n 中包含置换 π 的共轭类的势可以由下列公式表示:

$$\left|\pi^{S_n}\right| = \frac{n!}{1^r r! 2^s s! 3^t t! \cdots}.$$

6. 假设群 G 作用在集合 Ω 上. 子集 $\Gamma < \Omega$ 称为关于 G不变的 (或 G–不变的),如果对所有 $g \in G$ 和 $x \in \Gamma$, $gx \in \Gamma$. 例如, 同心环是 SO(2) 在 $\mathbb{R}^2$ 上作用的不变集.

证明, Ω 中的任意不变子集是一些轨道的并, 而且一个元素 $x \in \Omega$ 所在的 G–轨道正好是包含元素 x 的最小不变子群.

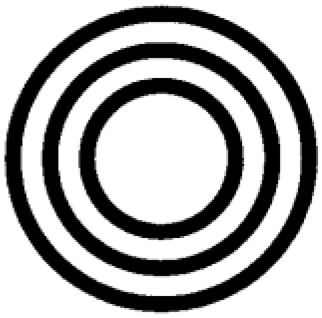


图 1

7. 证明, 对于群 G 和它的子群 H, 其作用 $H \times G \to G, (h, g) \mapsto hg$, 给出 G 关于 H 的右陪集分解.

8. 通过变动定理 1 的证明来得出关系

$$r(G:\Omega) = \frac{1}{|G|}\sum_{g\in G} N(g),$$

这里 $r(G:\Omega)$ 为作用在集合 Ω 上的置换群的轨道数.

9. (G. R. Goodson, 1999). 与群 G 的中心化子 $C(a) = \{x \in G | xa = ax\}$ 一样, 考虑在动力系统理论中遇到的反中心

$$D(a) = \{x \in G | xa = a^{-1}x\}.$$

一般说来, $D(a)$ 不是群.

证明:

1) $D(a)$ 是一个群当且仅当 $a^2 = e$ 且 $D(a) = C(a)$;

2) 集合 $E(a) = C(a) \bigcup D(a)$ 总是一个群.

§4 商群与同态

这一节, 尤其是第 2 目, 具有一定的难度, 而且对于它们需要重复数次, 以便通过具体的例子来掌握数量不多的抽象论断.

1. 商群的概念 群 G 关于正规子群的陪集所确定的 G 上的等价关系具有一个极好的性质. 即, 如果 a, b 是群的任意元且 $a \sim c, b \sim d$, 则通过运算有 $a^{-1}c = h_1 \in H, b^{-1}d = h_2 \in H$, 于是

$$(ab)^{-1}cd = b^{-1}a^{-1}cd = b^{-1}(a^{-1}c)d = b^{-1}h_1b(b^{-1}d) = h_1'h_2 \in H.$$

由此得到 $ab \sim cd$. 这里用到 H 在 G 中的正规性: $b^{-1}h_1b = h_1' \in H$. 因此

$$a \sim c, b \sim d \Longrightarrow ab \sim cd.$$

实际上, 这表明群 G 上的乘法运算诱导了商集合 $G/\sim$ 上的一个乘法运算, 我们将该商集合记为 G/H.

群 G 的任意两个子集 A, B 可以定义它们的合成 (关于乘法), 用 AB 表示所有元素积 ab 的集合, 其中 $a \in A, b \in B$. 由群 G 中的结合律推出

$$(AB)C = \{(ab)c\} = \{a(bc)\} = A(BC),$$

而 G 的一个子集 H 是 G 的一个子群当且仅当 $H^2 = H$ 且 $H^{-1} = \{h^{-1} | h \in H\} \subset H$.

从陪集角度看, aH 等于一个元素的集合 $\{a\}$ 与子群 H 的乘积. 两个陪集 aH, bH 的乘积是集合 $aH \cdot bH$, 一般讲, 它不一定是 H 的陪集. 在 §2, 我们看到的 S_3 关于 $H = \{e, (12)\}$ 的分解表明

$$H \cdot (13)H = (13)H \cup (23)H.$$

但完全有另一种情况, 当 H 为群 G 的一个正规子群时, 由于对所有的 $g \in G$, 我们有 $gH = Hg$, 所以

$$aH \cdot bH = a(Hb)H = a(bH)H = abH^2 = abH,$$

而且上面得到的论断说明, 陪集 abH 不依赖于陪集 aH, bH 的代表元的选取.

性质

$$aH \cdot bH = abH,$$
$$H \cdot aH = aH \cdot H = aH,$$
$$a^{-1}H \cdot aH = aH \cdot a^{-1}H = eH = H$$

表明下面定理成立.

定理 1 *如果 H 是 G 的一个正规子群, 那么乘法运算 $aH \cdot bH = abH$ 使商集合 G/H 成为一个群, 我们把它称为群 G 关于正规子群 H 的***商群***. 陪集 H 充当 G/H 的单位元, $a^{-1}H = (aH)^{-1}$ 是 aH 的逆元.*

当群 G 为有限群时, 商群 G/H 的阶可由下列公式计算:

$$|G/H| = \frac{|G|}{|H|} = (G : H).$$

此公式是由上面所论述的以及拉格朗日定理 (见 §2) 推得.

对于运算写为加法的交换群, 二元运算利用下列写法

$$(a + H) + (b + H) = (a + b) + H.$$

相应地, G/H 常常称为**群 G 模 H 的商群**, 而对于 $G = \mathbb{Z}, H = m\mathbb{Z}$ 的相应商群 G/H 一般也说成是 "群 $\mathbb{Z}$ 模 m 的商群".

2. 群的同态定理 由定理 1, 对于群 G 的每一个正规子群有那么一个新的群 G/K, 称之为 G 关于 K 的商群. 于是, 由第 1 节所描写的满同态 $\Phi: \mathrm{SU}(2) \to \mathrm{SO}(3)$, 自然地产生了商群 $\mathrm{SU}(2)/\{\pm E\}$, 其像 $\mathrm{Im}\,\Phi = \mathrm{SO}(3)$. 不难证明, $\mathrm{SU}(2)/\{\pm E\} \cong \mathrm{SO}(3)$, 但为了不要每一次都重新进行这些具体的讨论, 我们有必要建立子群的商、同态和商群的一般理论. 现在用 $K \lhd G$ 表示 K 是群 G 的一个正规子群.

定理 2 (同态基本定理) 设 $\varphi: G \to H$ 为群同态, 其核 $K = \mathrm{Ker}\,\varphi$. 那么 K 是 G 的一个正规子群且 $G/K \cong \mathrm{Im}\,\varphi$. 反之, 如果 $K \lhd G$, 那么存在一个群 H (也就是 G/K) 和满同态 $\pi: G \to H$, 其核等于 K.

(π 常称为自然映射或自然同态.)

证明 我们已经知道, $\mathrm{Ker}\,\varphi = K \lhd G$. 现在定义一个映射

$$\overline{\varphi}: G/K \to H, \quad \overline{\varphi}(gK) = \varphi(g).$$

如果 $g_1K = g_2K$, 那么 $g_1^{-1}g_2 \in K, \varphi(g_1^{-1}g_2) = e$, 于是 $\varphi(g_1) = \varphi(g_2)$. 这表明, 映射 $\overline{\varphi}$ 定义合理 (即它不依赖于陪集代表元的选取). 因为 $\overline{\varphi}(g_1K \cdot g_2K) = \overline{\varphi}(g_1gK) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \overline{\varphi}(g_1K)\overline{\varphi}(g_2K)$, 所以 $\overline{\varphi}$ 是一个同态. 而实际上 $\overline{\varphi}$ 是一个单同态, 这因为由 $\overline{\varphi}(g_1K) = \overline{\varphi}(g_2K)$ 推得 $\varphi(g_1) = \varphi(g_2)$, 从而 $\varphi(g_1^{-1}g_2) = e, g_1^{-1}g_2 \in K$, 即 $g_1K = g_2K$. 同样显然 $\mathrm{Im}\,\overline{\varphi} = \mathrm{Im}\,\varphi$.

反之, 假设 $K \lhd G$. 令 π 为一个函数, 它将 G 的每个元对应到 K 的一个陪集, 即 $\pi(g) = gK$. 显然, 它满足所有要求. □

应当指出, 不同的同态可能有相同的同态核, 例如, 阶 $p > 2$ 的交换群的自同态的 $g \mapsto g$ 和自同态 $g \mapsto g^{-1}$ 不同, 但它们的核相同 $(= e)$.

假如有同态 $\rho: G \to G_1$ 和子群 $H \subset G$, 自然地, 我们来看在 H 上的限制 $\rho|_H$ 一定是一个同态. 下列定理大大简化了所有可能情况的分析.

定理 3 (第一同构定理) 设 G 是一个群, H 和 K 是它的子群, 且 K 在 G 中正规, 那么 $HK = KH$ 为 G 的包含 K 的子群且 $H \cap K$ 是 H 的一个正规子群, 而映射

$$\varphi: hK \mapsto h(H \cap K)$$

是一个同构映射, 即

$$HK/K \cong H/H \cap K.$$

证明 由 $K \lhd G$, 我们得到 $gK = Kg, \forall g \in G$. 特别地, $hK = Kh$, 对于任意的 $h \in K$ 成立. 集合 $HK = \{hk | h \in H, k \in K\}$ 由一些陪集 hK 组成: $HK = \bigcup_{h \in H} hK$. 这里 $hK = Kh$, 于是我们有

$$HK = \bigcup_{h \in H} hK = \bigcup_{h \in H} Kh = KH.$$

显然, 单位元 e 属于 H, 也属于 K, 于是同样属于 HK. 进一步, $(hk)^{-1} = k^{-1}h^{-1} = h^{-1}(hkh^{-1})^{-1}$, 因而 HK 中所有元素的逆仍属于 HK. 此外, $HK \cdot HK = H \cdot KH \cdot K = H \cdot HK \cdot K = HK$, 即集合 HK 关于乘法封闭. 于是我们看到, 子集 $HK \subset G$ 是群 G 的一个子群.

因为 $K \subset HK$ 且 $K \lhd HK$, 所以我们有商群 HK/K. 令 $\pi : G \to G/K$ 为一个自然满同态, 且 $\pi_0 := \pi|_H$ 为 π 在 H 上的一个限制. 它的像 $\operatorname{Im}\pi_0$ 由陪集类 $hK, h \in H$, 组成, 即由所有代表元属于 H 的 G 关于 K 的所有陪集组成. 换句话说, $\operatorname{Im}\pi_0 = HK/K$. 于是, 我们有满同态

$$\pi_0 : H \to HK/K.$$

该同态的核 $\operatorname{Ker}\pi_0$ 由所有这样的 $h \in H$ 组成: 其满足 $\pi_0(h) = hK = K$ 为 HK/K 的单位元. 但是 $hK = K \Longleftrightarrow h \in H \cap K$, 于是 $\operatorname{Ker}\pi_0 = H \cap K$. 与任意同态核一样, $H \cap K$ 是群 H 的正规子群 (这可以没有困难地直接加以验证).

由同态基本定理 (定理 2), 对应 $\overline{\pi}_0 : h(H \cap K) \mapsto \pi_0(h) = hK$ 给出一个同构 $H/(H \cap K) \cong HK/K$. 因为 $\overline{\pi}_0$ 是一个一一对应, 所以 $\varphi := \overline{\pi}_0^{-1} : hK \mapsto h(H \cap K)$ 同样是 HK/K 到 $H/(H \cap K)$ 的一个同构映射. □

既然有第一同构定理, 就应该有第二同构定理. 它确实存在, 但我们宁愿表达为它的另一改善了的说法, 并用一个特别的名称.

定理 4 (对应定理) 假设 G 是一个群, H 和 K 是它的子群, $K \lhd G$ 且 $K \subset H$. 那么 $\overline{H} = H/K$ 是 $\overline{G} = G/K$ 的一个子群且 $\pi^* : H \mapsto \overline{H}$ 是群 G 中的包含 K 的子群集合 $\Omega(G, K)$ 到 $\overline{G}$ 的所有子群集合 $\Omega(\overline{G})$ 上的一个一一对应. 如果 $H \in \Omega(G, K)$, 那么 $H \lhd G \Longleftrightarrow \overline{H} \lhd \overline{G}$, 而且

$$G/H \cong \overline{G}/\overline{H} = (G/K)/(H/K).$$

证明 假设 $H \in \Omega(G, K)$. 由 G/K 的定义不难验证 H/K 是 G/K 的一个子群. 为了验证 $\pi^* : H \mapsto \overline{H}$ 的单射性, 我们来考虑满足 $H_1/K = H_2/K$ 的两个子群 $H_1, H_2 \in \Omega(G, K)$. 那么 $h_1 \in H_1 \Longrightarrow h_1K = h_2K, h_2 \in H_2 \Longrightarrow h_1 = h_2k$, 但因为 $K \subset H_2$, 所以 $h_1 \in H_2$, 从而 $H_1 \subset H_2$. 类似地可以证明 $H_2 \subset H_1$. 于是 $H_1 = H_2$.

现在我们来验证映射 π^* 是满射. 假设 $\overline{H} \in \Omega(\overline{G})$, 而 H 是 G 中所有那样的元的集合: 以它们为代表元的 K 的陪集为 $\overline{H}$. 那么, 由 $K \subset H$ 和 $a, b \in H \Longrightarrow aK, bK \in \overline{H} \Longrightarrow abK = aKbK \in \overline{H} \Longrightarrow ab \in H$, 且 $a \in H \Longrightarrow aK \in \overline{H} \Longrightarrow a^{-1}K = (aK)^{-1} \in \overline{H} \Longrightarrow a^{-1} \in H$. 这就是说, H 为 G 的一个子群, 且 $\overline{H} = H/K$ (通常人们称 H 为子群 $\overline{H} \subset \overline{G}$ 在 G 中的原像).

很显然由 $H \in \Omega(G, K)$ 和 $H \lhd G \Longrightarrow \overline{H} \lhd \overline{G}$, 实际上, 这因为 $gKhK \cdot (gK)^{-1} = ghg^{-1}K = h'K \in \overline{H}$, 对所有 $g \in G, h \in H$ 成立. 同样的推理, $\overline{H} \lhd \overline{G} \Longrightarrow ghg^{-1}K = gK \cdot hK \cdot (gK)^{-1} = h'K \Longrightarrow ghg^{-1} \in H \Longrightarrow H \lhd G$.

最后, 当 $H \in \Omega(G,K), H \lhd G$ 时, 由上面已证明的, 可以看两个自然同态

$$\pi: G \to G/K, \quad \overline{\pi}: \overline{G} \to \overline{G}/\overline{H}$$

$(\overline{g} \mapsto \overline{\pi}(\overline{g})$, 这里$\overline{g} = gK \in \overline{G})$ 以及它们的合成

$$\sigma = \overline{\pi} \circ \pi : G \to \overline{G}/\overline{H},$$

其定义规则为 $\sigma(g) = \overline{\pi}(\overline{g}) = \overline{g}\overline{H}$. 则我们有

$$\begin{aligned}\operatorname{Ker}\sigma &= \{g \in G | \sigma(g) = \overline{H}\} = \{g \in G | \overline{g} \in \overline{H}\} \\ &= \{g \in G | gK = hK, \text{对于某一个 } h \in H\} = H.\end{aligned}$$

于是, 由同态基本定理, 映射 $gH \mapsto \overline{g}\overline{H}$ 是群 G/H 与 $\overline{G}/\overline{H}$ 之间的一个同构映射.

□

例 1 设 $n = dm$ 为具有一个因子 $d > 1$ 的自然数. 显然 $n\mathbb{Z} \subset d\mathbb{Z}$, 且映射 $x \mapsto dx + n\mathbb{Z}$ 是加群的满同态:

$$\mathbb{Z} \to d\mathbb{Z}/n\mathbb{Z} = \{di + n\mathbb{Z} | i = 0, 1, \cdots, m-1\},$$

其核为 $m\mathbb{Z}$. 由定理 2 有同构

$$Z_m := \mathbb{Z}/m\mathbb{Z} \cong d\mathbb{Z}/n\mathbb{Z}$$

(这很容易理解). 利用定理 4, 有

$$\mathbb{Z}/d\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z})/(d\mathbb{Z}/n\mathbb{Z}),$$

即 $Z_d \cong Z_n/Z_m$.

由拉格朗日定理, 我们得出断言: 循环群的所有子群和商群还是循环群.
这个结果当然可以不用同态定理得出.

例 2 在对称群 S_4 中选出子群

$$\begin{aligned}V_4 &= \{e, (12)(34), (13)(24), (14)(23)\} \lhd S_4, \\ S_3 &= \{e, (12), (13), (23), (123), (132)\}\end{aligned}$$

(这里 S_3 为点 $i = 4$ 的稳定子群). 因为, 显然 $S_3 \cap V_4 = e$, 所以对于子群 $H = S_3V_4$, 由定理 3 有

$$H/V_3 \cong S_3/(S_3 \cap V_4) \cong S_3.$$

特别地, $|H| = |V_4| \cdot |S_3| = 24$, 于是 $H = S_4$. 这表明, S_4 有同构于 S_3 的子群和商群. 由定理 4, 我们得到 S_4 的包含 V_4 的子群集合 $\Omega(S_4, V_4)$ 的描写:

$$\Omega(S_4, V_4) = \{V_4, \langle(12)\rangle V_4, \langle(13)\rangle V_4, \langle(23)\rangle V_4, A_4 = \langle(123)\rangle V_4, S_4\}.$$

我们将注意力转到这样的情形, 对于数 24 的任一因子 d, S_4 至少有一个 d 阶子群. 特别是它恰有 4 个阶为 3 的子群 $\langle(123)\rangle, \langle(124)\rangle, \langle(134)\rangle, \langle(234)\rangle$ 和 3 个 8 阶子群 $\langle(12)\rangle V_4, \langle(13)\rangle V_4, \langle(23)\rangle V_4$ (它们分别称为 S_4 的西罗 3–子群和西罗 2–子群). 不等于 S_4 本身的正规子群共有两个: V_4 和 A_4.

事实上, 如果 $K \lhd G$ 且 $K \cap V_4 \neq e$, 那么 $K \supset V_4$, 这因为 V_4 中的非单位元在 S_4 中互相共轭. 于是由集合 $\Omega(S_4, V_4)$ 我们看到, $K = V_4$ 或 $K = A_4$. 而如果 $K \cap V_4 = e$ 且 $K \neq e$, 那么

$$K \lhd S_4, V_4 \lhd S_4 \Longrightarrow KV_4 \lhd S_4,$$

而这只能是 $KV_4 = S_4$, 从而 $K \cong S_3$. 但 S_3 包含对换, 而所有对换在 S_4 中互相共轭且生成 S_4. 另一方面, 它们应该含于 K. 得到的矛盾表明, $K \cap V_4 = e$ 不可能.

3. 换位子群　表达式

$$(x, y) = xyx^{-1}y^{-1}$$

称为群 G 的元素 x, y 的**换位子**, 它起着为了交换 x 和 y 的位置的校正作用:

$$xy = (x, y)yx.$$

如果 x 和 y 可交换, 那么 $(x, y) = e$. 直观地看出, 群 G 中不等于 e 的换位子越多, 那么群 G 中乘法离可换就越远. 记 M 为 G 的所有换位子的集合, 人们称由集合 M 生成的子群 $G'(= G^{(1)} = (G, G))$ 为群 G 的**换位子群** (**或导出子群**) (参见 [BA I], 第 4 章 §2 习题 1,2):

$$G' = \langle (x, y) | x, y \in G \rangle := \mathrm{gr}(x, y).$$

虽然 $(x, y)^{-1} = yxy^{-1}x^{-1} = (y, x)$ 仍是一个换位子, 但两个换位子的乘积不一定是换位子, 于是 G' 由所有可能的乘积形式

$$(x_1, y_1)(x_2, y_2) \cdots (x_k, y_k), \quad x_i, y_i \in G$$

组成.

当然, 在每个具体的情况下, 对换位子群 G' 希望有更好的描写.

例 3　假设 $G = S_n$. 对于 S_n 中任意两个元素 α, β 的换位子 $(\alpha, \beta) = \alpha\beta\alpha^{-1}\beta^{-1}$ 显然是一个偶置换, 于是 $S_n' \subset A_n$. 进一步,

$$(ij)(ik)(ij)^{-1}(ik)^{-1} = (ij)(ik)(ij)(ik) = (ijk),$$

而因为 3 循环 (ijk) 生成整个交错群 A_n (参见 [BA I], 第 4 章 §2 习题 11), 因此我们不得不有 $S_n' = A_n$.

我们注意, $S_n' \lhd S_n$, 而商群 S_n/S_n' 是交换群.

现在回到一般情况, 我们来看看任意群同态 $\varphi: G \to \overline{G}$. 因为

$$\varphi((x,y)) = \varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1},$$

所以 $\varphi(G') \subset (\overline{G})'$, 且如果 φ 为满同态, 则 $\varphi(G') = (\overline{G})'$. 令 K 是群 G 的一个正规子群且 $\varphi = I_a : x \mapsto axa^{-1}$ 为群 G 的内自同构, 它在 K 上诱导一个自同态. 由上面所说的, 对任意 $a \in G$, 有 $I_a(K') \subset K'$, 但这意味着

$$K \lhd G \Longrightarrow K' \lhd G. \tag{1}$$

特别地, $G' \lhd G$.

现在我们证明更一般的结论, 它揭示了换位子群概念的内在意义.

定理 5 任意一个子群 $K \subset G$, 如果 K 包含群 G 的换位子群 G', 则 K 在 G 中正规. 商群 G/G' 是交换的, 而 G' 含于每个使其商群 G/K 交换的正规子群 K 中 (特别地, 交换商群 G/K 最大阶等于指数 $(G:G')$).

证明 如果 $x \in K, g \in G$ 且 $G' \subset K$, 那么 $gxg^{-1} = (gxg^{-1}x^{-1})x = (g,x)x \in G'K = K$, 于是 $K \lhd G$. 再由条件 $G' \subset K, K \lhd G$ (当 $K = G'$ 时同样适合), 我们有

$$(aK, bK) = aK \cdot bK \cdot a^{-1}K \cdot b^{-1}K = aba^{-1}b^{-1}K = (a,b)K = K,$$

即商群 G/K 的任何两个元的换位子等于单位元 $(= K)$. 这就是说, G/K 是交换群. 反之, 如果 $K \lhd G$ 且商群 G/K 交换, 那么

$$(a,b)K = (aK, bK) = K,$$

对所有的 $a, b \in G$. 于是 $(a,b) \in K$, 从而 $G' \subset K$, 这因为 G' 由所有的换位子生成.

□

注 我们现在已经知道了任意群 G 有两个重要的正规子群: 中心 $Z(G)$ 和换位子群 G'. 与它们相联系, 一般地讲, 一个较弱的但更一般的规律是: G 离交换群越近, 那么 $Z(G)$ 越大而 G' 越小. 更有趣的是下列事实.

非交换群 G 关于中心 $Z(G)$ 的商群 $G/Z(G)$ 不可能是循环群.

事实上, 如果 $G/Z(G)$ 是循环群, 那么 $G = \bigcup_i a^i Z(G)$, 从而 G 中任意元可以写为形式 $g = a^i z, z \in Z(G)$. 于是 $(g,h) = (a^i z, a^j z') = a^{i+j-i-j}(z,z') = e$, 对于任意两个元 $g, h \in G$. 这表明 $G' = e$, 从而 G 是一个交换群, 这与假设矛盾. □

4. 群的积 我们现在来研究利用给定群来构造新的群. 在各种个别的现象中, 我们已经碰到这种结构. 设 A, B 为任意两个群. 令 $A \times B$ 为所有有序元素对 (a,b)

(不要将它与换位子搞混) 的集合, 其中 $a \in A, b \in B$, 在 $A \times B$ 上引进二元运算

$$(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2).$$

则称 $A \times B$ 为群 A 和群 B 的 (**外**) **直积**. 严格地说, 应当写成 $(a_1, b_1) * (a_2, b_2) = (a_1 \circ a_2, b_1 \diamond b_2)$, 这里 $\circ, \diamond, *$ 分别为 A, B 和 $A \times B$ 的二元运算, 但是, 对所有运算的写法, 我们只用符号 ——“·” 来表示 (不过, 我们又省略了它). 对于写成加法的群, 例如交换群, 自然地, 有所谓的直和 $A \oplus B$.

在直积 $A \times B$ 中包含两个子群 $A \times e$ 和 $e \times B$, 它们分别同构对应于 A 和 B (还有一个习惯: A 和 B 的单位元都用一个符号 e 表示). 令映射 $\varphi : A \times B \to B \times A$, 其元素对应为 $\varphi((a, b)) = (b, a)$, 显然, 它是群 $A \times B$ 与群 $B \times A$ 的同构映射, 如果我们有 3 个群 A, B, C, 那么可以有直积 $(A \times B) \times C$ 和 $A \times (B \times C)$. 令 $\psi(((a, b), c)) = (a, (b, c))$, 那么容易验证

$$(A \times B) \times C \cong A \times (B \times C).$$

直积的交换性和结合性允许我们谈论任意有限多个群 $G_1, G_2, \cdots, G_n$ 的直积, 并写为

$$G_1 \times G_2 \times \cdots \times G_n = \prod_{i=1}^{n} G_i, \tag{2}$$

这里我们没有用括号标出两两直积的次序 (我们正好将所有群的集合变成了一个半群, 其元素为群).

定理 6 *假设 G 为一个群, 它有两个正规子群 A 和 B. 如果 $A \cap B = e$ 且 $AB = G$, 则 $G \cong A \times B$.*

证明 由等式 $G = AB$, 我们有, 对任意元 $g \in G$, 可以写为形式 $g = ab$, 其中 $a \in A, b \in B$. 如果还有 $g = a_1b_1, a_1 \in A, b_1 \in B$, 那么 $ab = a_1b_1 \Longrightarrow a_1^{-1}a = b_1b^{-1} \in A \cap B = e$. 于是 $a_1 = a, b_1 = b$. 这表明 $g = ab$ 的写法是唯一的. 又因为, $A \lhd G \Longrightarrow k = a(ba^{-1}b^{-1}) = aa' \in A; B \lhd G \Longrightarrow k = (aba^{-1})b^{-1} = b'b^{-1} \in B$, 所以换位子 $k \in A \cap B = e$ 为单位元, 由此得到 $ab = ba$.

我们现在定义一个映射 $\varphi : G \to A \times B$, 其元素对应为对于任意 $g = ab, \varphi(g) = (a, b)$. 由上面的讨论, $\varphi(gg') = \varphi(aba'b') = \varphi(aa'bb') = (aa', bb') = (a, b)(a', b') = \varphi(ab)\varphi(a'b') = \varphi(g)\varphi(g')$. 另外, $\varphi(ab) = (e, e) \Longleftrightarrow a = e, b = e$, 即 $\operatorname{Ker}\varphi = e$. 而 φ 是满射是显然的. 因此 φ 满足群同构映射的所有性质. □

满足定理 6 的条件的群 G 称为它的子群 A 和 B 的 (**内**) **直积**. 与外直积不同之处在于群 G 包含的直因子是 A, B, 而不是与它们同构的 $A \times e, e \times B$. 当然, 外直积 $G = A \times B$ 也是它的子群 $A \times e$ 和 $e \times B$ 的内直积, 于是我们可以对它们不加区分, 并简称为 “直积”.

下列定理给出了有关直积的同态的一些信息.

定理 7 设 $G = A\times B$, 且 $A_1 \lhd A, B_1 \lhd B$. 那么 $A_1\times B_1 \lhd G$ 且 $G/(A_1\times B_1) \cong (A/A_1)\times(B/B_1)$. 特别地, $G/A \cong B$.

证明 令 $\alpha: A \to A/A_1$, 且 $\beta: B\to B/B_1$ 为两个自然同态. 定义映射 $\varphi: G\to (A/A_1)\times(B/B_1)$, 其元素对应为 $\varphi(a,b) = (\alpha(a),\beta(b))$. 直接验证知, φ 是一个同态映射, 其核 $\operatorname{Ker}\varphi = A_1\times B_1$, 而像 $\operatorname{Im}\varphi = (A/A_1)\times(B/B_1)$. □

就像向量空间的理论一样, 容易证明, 如果群 G 有正规子群 $G_1,\cdots,G_n$, 那么 $G\cong \prod\limits_i G_i$ 的充分必要条件是对于所有 j, 有

$$G = \langle G_1,\cdots,G_n\rangle \text{ 且 } G_j \cap \langle G_1,\cdots,\widehat{G}_j,\cdots,G_n\rangle = e$$

(在 G_j 上加一个 "帽子" 表示分量 G_j 不出现). 这本身就说明了下列性质: 如果 G 的每个元 g 能够写成形式 $g = g_1\cdots g_n, g_i\in G_i$ 且该写法是唯一的, 那么 G 是它的正规子群 $G_1,\cdots,G_n$ 的直积. n 个群 H 的直积也称为群 H 的直 n 次幂, 记为 $H^n = H\times\cdots\times H$. 在 H^n 中有一个特殊的子群 $\Delta = \{(h,h,\cdots,h)|h\in H\}$ 称为对角线子群, 它同构于 H.

如果在定理 6 中去除 $B\lhd G$ 的条件, 那么我们得到**半直积**的概念: $G = AB, A\cap B = e, A\lhd G$ (有时将该半直积写为 $G = A\leftthreetimes B$). 由这个定义随之引起了子群 B 在正规子群 A 上同构作用的描写, 这通常发生在每个具体的群中.

注 许多对于我们熟悉的群都能写成直积和半直积的形式. 例如, S_n 是它的正规子群 A_n 和 2 阶循环子群 $\langle(12)\rangle$ 的半直积: $S_n\cong A_n\leftthreetimes Z_2$. 利用第 2 目中例 2 的记号, 可以写

$$A_4 = V_4\leftthreetimes\langle(123)\rangle \cong (Z_2\times Z_2)\leftthreetimes Z_3,$$
$$S_4 = V_4\leftthreetimes S_3 \cong (Z_2\times Z_2)\leftthreetimes(Z_3\leftthreetimes Z_2).$$

再一个例子: 仿射变换 $\mathbb{R}\to\mathbb{R}$ 构成的群 (参见 [BA I], 第 4 章或 [BA II]) 是一个平移的正规子群与保持点 $x=0$ 不变的变换组成的子群 $\mathrm{GL}(1,\mathbb{R})$ 的半直积.

5. 生成元与定义关系 关于群 G 的生成系的问题已经在 [BA I] 第 4 章讨论过. 为了用新的观点来看一些我们熟悉的群, 我们现在重新回到这个问题. 由 [BA I], 第 4 章的结果推得, 对于循环群没有必要考虑庞大的凯莱表. 下列式子

$$C_n = \langle c|c^n = e\rangle \tag{3}$$

给出了阶为 n 的抽象循环群 C_n 所有必要的信息; 这指的就是, $C_n = \{e,c,c^2,\cdots,c^{n-1}\}$, 且当 $s+t<n$ 时 $c^sc^t = c^{s+t}$, 而当 $s+t\geqslant n$ 时, $c^sc^t = c^{s+t-n}$. 另一方面, 准确到同构, 任意循环群都是群 $(\mathbb{Z},+)$ 的同态像.

现在假设 F_n 为具有单位元 e 且由 n 个生成元 $f_1, \cdots, f_n$ 生成的一个群, 其每个元 f 可以写成 (可能有许多写法) 表达式

$$f = f_{i_1}^{s_1} f_{i_2}^{s_2} \cdots f_{i_k}^{s_k}, i_j \in \{1, 2, \cdots, n\}, \quad s_j \in \mathbb{Z}, \tag{4}$$

这里 $i_j \neq i_{j+1}, j = 1, 2, \cdots, k-1$. 下列初等关系总成立:

$$f_i^s \cdot f_i^t = f_i^{s+t}, \quad f_i^0 = e \quad 且 \quad f_j e = e f_j = f_j.$$

如果满足条件: $f = e \iff s_1 = \cdots = s_k = 0$, 对每个写成表达式 (4) 的 f, 则称 F_n 是一个由 n 个自由生成元生成的秩为 n 的自由群. 群 F_n 中的元素通常称为在字母表 $\{f_1, f_1^{-1}, \cdots, f_n, f_n^{-1}\}$ 中的字. 字 f 的不可约表达式 (4) 和它的长 $l(f) = |s_1| + |s_2| + \cdots + |s_k|$ 被唯一确定; 否则空字 $e := \varnothing = ff^{-1}$ (F^n 的单位元) 就会有长 > 0. 对于给定的 n, 两个分别由自由生成元 $f_1, \cdots, f_n$ 和 $g_1, \cdots, g_n$ 生成的自由群 F_n 和 G_n 是同构的; 这只需令 $\Phi(f_i) = g_i, 1 \leqslant i \leqslant n$, 而对表达式为 (4) 的字 f, 让

$$\Phi(f) = g_{i_1}^{s_1} g_{i_2}^{s_2} \cdots g_{i_n}^{s_n}$$

(F_n 和 G_n 的单位元用同一个记号表示). 但是, 如果 G_n 不是自由群, 那么 Φ 将仅仅是一个满同态, 其核 $\mathrm{Ker}\Phi$ 为由 F_n 中所有这样的字组成, 其在代换 $f_i \mapsto g_i$ 下变为 G_n 的单位元. 这一通用的性质 (即将 $f_i \mapsto g_i, 1 \leqslant i \leqslant n$ 使 $\Phi: F_n \to G_n$, 对于任意具有 n 个生成元的群 G_n, 为满同态的可能性) 可以作为自由群 F_n 的定义, 但我们不在此耽搁了.

为了使自由群不被觉得是 "神秘的对象", 我们讨论几个具体的情况.

$n = 1, F_1 \cong (\mathbb{Z}, +)$ 是秩为 1 的自由交换群, 也就是无限循环群.

$n = 2$, 令 $\mathbb{Z}[t]$ 为具有整有理系数的关于 t 的多项式环. 在特殊线性群 $\mathrm{SL}(2, \mathbb{Z}[t])$ 中, 我们来考虑由矩阵

$$A = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$$

生成的子群 F. 我们证明 F 是一个自由群. 对 k 进行归纳容易证明, 元素

$$W_k = A^{\alpha_1} B^{\beta_1} \cdots A^{\alpha_k} B^{\beta_k}, \quad \alpha_i, \beta_i \neq 0, \quad 1 \leqslant i \leqslant k$$

有形式

$$W_k = \begin{pmatrix} 1 + \cdots + \sigma_k t^{2k} & t\left(\cdots + \sigma_{k-1} \alpha_k t^{2(k-1)}\right) \\ t\left(\cdots + \alpha_1^{-1} \sigma_k t^{2(k-1)}\right) & 1 + \cdots + \alpha_1^{-1} \sigma_{k-1} \alpha_k t^{2(k-1)} \end{pmatrix},$$

其中 $\sigma_k = \alpha_1 \beta_1 \cdots \alpha_k \beta_k$, 而点 "$\cdots$" 表示次数小于 t 的单项式. 显然 $W_k \neq E$. 群 F 的任意元可以写成或者 $B^\beta A^\alpha \neq E$ 或者 $W = B^\beta W_k A^\alpha$. 如果 $W = E$, 那么 $W_k = B^{-\beta} A^{-\alpha}$, 这显然是不可能的 (在 $k > 1$ 时比较它们的次数, 而当 $k = 1$, 验证是直接的).

一个不大的补充推论是, 如果让 $t = m$, 这里 m 为 $\geqslant 2$ 的任一整数, 则群 F 仍是自由的.

现在我们引入下列

定义 令 F_n 为具有 n 个自由生成元 $f_1, \cdots, f_n$ 的自由群, $S = \{W_i, i \in I\}$ 为元素 $W_i(f_1, \cdots, f_n) \in F_n$ 的某一子集合, 且 $K = \langle S^{F_n} \rangle$ 为包含 S 的 F_n 的最小正规子群 (即包含 S 的所有正规子群的交). 称群 G 为由 n 个生成元 $a_1, \cdots, a_n$ 和定义关系 $W_i(a_1, \cdots, a_n) = e (i \in I)$ 所确定的, 如果存在一个核为 K 的满同态 $\pi : F_n \to G$ 满足 $\pi(f_k) = a_k, 1 \leqslant k \leqslant n$. 在这种情况下, 记

$$G = \langle a_1, \cdots, a_n | W_i(a_1, \cdots, a_n) = e, i \in I \rangle.$$

如果 $\operatorname{Card} I < \infty$, 则称 G 为**有限定义的群**.

自由群 F_n 本身是 “没有定义关系” 的, 这也就是它被称为 “自由” 称号的原因. 由定义可以看出, 任一个具有 n 个生成元 $b_1, \cdots, b_n$ 且同样满足关系 $w_i(b_1, \cdots, b_n) = e, i \in I$, 也许还满足其它一些关系的群 H 是群 G 的同态像. 特别地, $|H| \leqslant |G|$. 一般地说, 利用生成元和定义关系可以来决定群, 但是对于具体的群做起来并不容易. 最实质的问题是在于不存在一般的算法, 使得能够对于任意有限定义的群, 回答有关群的有限性的问题, 它们的字相等的问题, 等等. 在这方面, 发展了组合群论的丰富内容. 我们暂时来看两个内容丰富的例子, 这里所有提到的问题被完全解决了.

例 1 (二面体群) 群 $G = \langle a, b | a^3 = b^2 = abab = e \rangle$ 具有两个生成元和三个定义关系. G 的阶 $|G| \leqslant 6$, 这因为在 G 中 $ba = a^{-1}b^{-1} = (a^3)^{-1}a^2b(b^2)^{-1} = a^2b$. 所以在任何情况下, G 最多具有这样一些元 e, a, e^2, b, ab, a^2b. 因为生成 S_3 的两个置换 $(123), (12)$ 满足关系 $(123)^3 = (12)^2 = (123)(12)(123)(12) = e$, 所以映射 $\varphi : G \to S_3$, 其元素对应为 $a \mapsto (123), b \mapsto (12)$, 给出同构 $G \cong S_3$. 于是对称群 S_3 被两个生成元和 3 个定义关系所确定. 回想, S_3 也同样可以看作三角形的对称变换.

正 n 边形 P_n 的对称变换的完全群称为**二面体群**, 并用符号 D_n 表示. 平面上绕置于直角坐标系的原点 O 为中心, 转角为 $\theta = \dfrac{2\pi}{n}$ 的旋转

$$\mathcal{A} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

产生一个阶为 n 的循环群 $\langle \mathcal{A} \rangle$. 在 D_n 中还包含一个多边形 P_n 关于过原点和一个顶点的轴的一个反射 (见图 2).

$$\mathcal{B} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

由定义知 $\mathcal{B}^2 = e$. $2n$ 个不同的对称变换

$$e, \mathcal{A}, \mathcal{A}^2, \cdots, \mathcal{A}^{n-1}, \quad \mathcal{B}, \mathcal{AB}, \cdots, \mathcal{A}^{n-1}\mathcal{B} \tag{5}$$

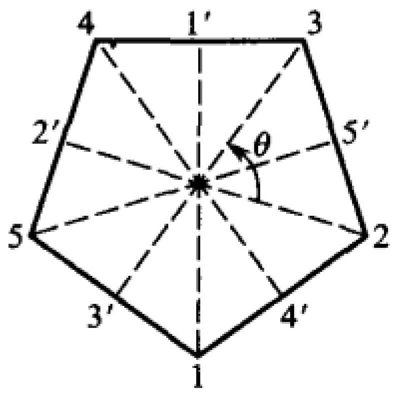


图 2

穷尽整个群. 于是, 任一对称变换被它在多边形 P_n 的顶点 $1, 2, \cdots, n$ 上的作用所确定. 如果哪个变换将 1 变到 k, 那么它或者保持刚才所说的那种点的循环次序, 就如 $\mathcal{A}^k$ 的作用, 或者反过来变到它, 就如 $\mathcal{A}^{k-1}\mathcal{B}$ 的作用.

因此在 D_n 中除了 (5) 中的元之外, 没有其它的元. 我们指出, 变换 $\mathcal{BA}$ 等于 $\mathcal{A}^{n-1}\mathcal{B}$, 因为这两个变换都将点 1 变为 n. 于是, 我们有

$$\mathcal{A}^n = e, \quad \mathcal{B}^2 = e, \quad \mathcal{ABAB} = e.$$

这表明 D_n 是群

$$G = \langle a, b | a^n = b^2 = abab = e \rangle$$

的同态像. 但是, 当 $n = 3$ 时, 我们有 $ba = a^{n-1}b$, 于是字母表 $\{a, a^{-1}, b, b^{-1}\}$ 组成的任一字可简化为 a^i 或 $a^ib, 0 \leqslant i \leqslant n-1$. 因此 $|G| \leqslant 2n$, 但由上面所说的可以看到 $G \cong D_n$, 这本身得到了二面体群的生成元和定义关系的表达式. 把 G 与 D_n 看作相同:

$$D_n = \langle a, b | a^n = e, b^2 = e, (ab)^2 = e \rangle.$$

因为 $\langle a \rangle \lhd D_n$ 且 $D_n/\langle a \rangle$ 是一个循环群, 那么应用定理 4, 对于群 D_n 的换位子群, 有 $D_n' \subset \langle a \rangle$. 但是因为 $a^2 = aba^{-1}b^{-1} = (a, b) \in D_n'$, 所以当 n 为奇数时, $D_n' = \langle a \rangle$, 而当 n 为偶数时, $D_n/\langle a^2 \rangle = \langle \bar{a}, \bar{b} \rangle$ 为两个 2 阶循环群的直积, 于是 $D_n' = \langle a^2 \rangle$. 群 D_n 的中心 $Z(D_n)$ 和它的共轭类的个数 r 同样取决于 n 的奇偶性. 我们有下表 (很容易验证):

当 $n = 2m$, 则 $D_n' = \langle a^2 \rangle, (D_n : D_n') = 4, Z(D_n) = \langle a^m \rangle, r = m + 3$,

1	1	2	$\cdots$	2	m	m
e	a^m	a	$\cdots$	a^{m-1}	b	ab

若 $n = 2m + 1$, 则 $D_n' = \langle a \rangle, (D_n : D_n') = 2, Z(D_n) = e, r = m + 2$,

1	2	$\cdots$	2	2	n
e	a	$\cdots$	a^{m-1}	a^m	b

下行所列为共轭类的代表元, 上行为共轭类的势.

值得强调的是, 定义关系的形式 (即 $w_i = e$ 的左边) 依赖于群的生成系的选取, 例如, 二面体群 D_n 被任意两个相交角为 π/m 的直线反射生成. 因而

$$D_n = \langle g_1, g_2 | g_1^2 = g_2^2 = (g_1 g_2)^n = e\rangle.$$

如果出发点是以前的表达式, 那么可以令 $g_1 = ab, g_2 = b$.

例 2 (四元数群) 与上面例子不同, 我们一开始就用生成元和定义关系来定义四元数群:

$$Q_8 = \langle a, b | a^4 = e, b^2 = a^2, bab^{-1} = a^{-1}\rangle.$$

又 $ba = a^{-1}b = a^3 b$, 且因为 $b^2 = a^2$, 任意字母表 $\{a, a^{-1}, b, b^{-1}\}$ 的字可写成 $a^s b^t, 0 \leqslant s \leqslant 3, 0 \leqslant t \leqslant 1$, 于是 $|Q_8| \leqslant 8$.

我们能否确认 $|Q_8| = 8$ 呢? 是的, 但这首先需要我们给出一个 8 元群, 它有两个生成元分别对应到 a 和 b. 由 §1 习题 3 我们知道, 由四元数单位 $\mathbf{i}, \mathbf{j}, \mathbf{k}$ 就产生这样的群, 同样由下列矩阵也产生这样的群

$$A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad (i = \sqrt{-1}).$$

事实上, $A^4 = E, B^2 = A^2, BAB^{-1} = A^{-1}$,

$$\langle A, B\rangle = \left\{\pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \pm\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}\right\}.$$

这些矩阵我们已经在 §1 练习 3 中碰到过. 事实上, 映射 $a \mapsto A, b \mapsto B$ 就是 Q_8 到 $\langle A, B\rangle$ 的一个同构映射, $Q_8 \cong \langle A, B\rangle$. 我们指出, $a^2 \in Z(Q_8)$, 而因为非交换群关于中心的商群不是一个循环群 (参见定理 5 证明后面的注), 所以 $\langle a^2\rangle = Z(Q_8)$. 因为所有 4 阶群为交换群, 所以 $Q_8/Z(Q_8) \cong V_4$ 是两个 2 阶循环群的直积. 于是, 换位子群 Q_8' 等于 $Z(Q_8)$ 且 $(Q_8 : Q_8') = 4$. 有关共轭类的信息包含在下表中:

1	1	2	2	2
e	a^2	a	b	ab

有限定义的群 (它们最简单的例子我们已经看到) 出现在各种不同的数学领域, 例如, 所谓的基本群流形. 不足为怪, 还有许多与它们有关的问题等待去发现.

习 题

1. 回忆在 [BA I] 第 4 章 §2 第 4 目中关于内自同构 $I_a : g \mapsto aga^{-1}$ 和内自同构群 $\mathrm{Inn}(G) \subset \mathrm{Aut}(G)$ 的定义. 证明, $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$ 且 $\mathrm{Inn}(G) \cong G/Z(G)$, 其中 $Z(G)$ 为群 G 的中心. 商群 $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ 称为群 G 的外自同构群.

2. 假设 H 和 K 是群 G 的子群, 证明

$$|HK|\cdot|H\cap K|=|H|\cdot|K|.$$

(大家知道, 在线性空间理论中也有类似的公式). 进一步证明, 集合 HK 为子群的充分必要条件是 $HK=KH$; 特别地, 当 $K\lhd G$ 时, 这个条件自然满足.

3. 对于对称群 S_4 编制类似于上面刚刚讲到的例子中的表格

1	3	6	8	6
e	(12)(34)	(12)	(123)	(1234)

仅仅依据一个明显的事实, 即在任意群中, 一个正规子群是一些共轭类的并, 来重新描述例 2 中所说的 S_4 的正规子群.

4. 证明: $Z(A\times B)=Z(A)\times Z(B)$.

5. 如果 $K_1,K_2\lhd G, K_1\cap K_2=e$, 那么 G 同构于 $(G/K_1)\times(G/K_2)$ 的一个子群. 该命题正确吗?

6. 假设 $K\lhd G=A\times B$. 证明, 或者 K 是交换群, 或者 $K\cap A$ 和 $K\cap B$ 中有一个非平凡. 给出一个例子说明在群 $A\times B$ 中有一个非平凡的正规子群 K 满足 $K\cap A=e$ 且 $K\cap B=e$. 这本身也说明了, 由 $K\lhd A\times B$, 一般而言, 不能推得 $K=(K\cap A)\times(K\cap B)$.

7. 四元数群 Q_8 是不是它的某两个真子群的半直积?

8. 证明, 对于任意真子群 $H\subset Q_8$, 有 $H\lhd Q_8$.

9. 证明, 群 D_4 与 Q_8 不同构.

10. 证明, $\mathrm{Aut}(D_4)\cong D_4$ (因为 $|Z(D_4)|=2$, 所以, 由练习 1, $|\mathrm{Out}(G)|=2$).

11. 全体 p^i 次单位根的集合, $i=0,1,2,\cdots$, 构成一个无限群 $C(p^\infty)$. 它被称为*拟循环群*, 因为它的任意有限个元生成一个循环群. 试验证这一点, 同时证明

$$C(p^\infty)=\langle a_1,a_2,a_3,\cdots|a_1^p=1,a_{i+1}^p=a_i,\quad i=1,2,3,\cdots\rangle.$$

12. (J. Monthly, 80, №. 9, 1973). 设

$$G=\langle a,b|aba=ba^2b,a^3=e,b^{2n-1}=e\rangle,$$

其中 $n\in\mathbb{N}$. 证明, $n=1$, 即 $b=e$ 且实际上 $G=\langle a|a^3=e\rangle$ 为一个 3 阶循环群.

13. 建立一个单一同态 $f:S_n\to\mathrm{GL}(n)$ 满足矩阵 $f(\pi)$ 的行列式 $\det f(\pi)=\varepsilon_\pi,\pi\in S_n$.

形如 $f(\pi),\pi\in S_n$ 的矩阵称为**置换矩阵**. f 在 A_n 上的限制是到 $\mathrm{SL}(n,\mathbb{R})$ 内的单一同态. 映射 $L:G\to S_n$ (凯莱定理) 与 $f:S_n\to\mathrm{GL}(n)$ 的合成 $f\circ L$ 变成 $G\to\mathrm{GL}(n)$ 的一个单一同态, 对于任意有限群 G.

试具体写出 $n=3$ 时的映射 f 的明显形式.

14. 补充下列形式定义的 n 秩**自由群** F_n 的细节. 字母表 $A=\{a_1,a_1^{-1},\cdots,a_n,a_n^{-1}\}$ 由 n 个字母 $a_1,\cdots,a_n$ 和它们的 "对映点" $a_1^{-1},\cdots,a_n^{-1}$ 组成, 再添加一个符号 $e:=\varnothing$. 令 S 为这 $2n+1$ 个符号以任何次序写成的有限长的所有 "字" 的集合. 在字里允许有重复出现的符号.

两个字 u 和 v 的**积** uv 认为是字 u 在前 v 在后的组成字. 字 $u^{-1}=a_{i_m}^{-\varepsilon_m}\cdots a_{i_1}^{-\varepsilon_1}$ 称为字 $u=a_{i_1}^{\varepsilon_1}\cdots a_{i_m}^{\varepsilon_m},\varepsilon_i=\pm1,k=1,\cdots,m$ 的**逆**, $e^{-1}=e$. 在 S 上引进一个等价关系 $\sim$. 两个字认为是等价的, 如果其中一个可以由另一个通过有限次下列等价变换得到:

$$\begin{aligned} &ee\sim e,\\ &a_ia_i^{-1}\sim e,\qquad a_i^{-1}a_i\sim e,\\ &a_ie\sim a_i,\qquad a_i^{-1}e\sim a_i^{-1},\\ &ea_i\sim a_i,\qquad ea_i^{-1}\sim a_i^{-1}.\end{aligned}$$

在每个等价类中包含唯一一个 "不可约的" (最短的) 字. 在由等价关系 $\sim$ 确定的等价类集合上由字的乘法诱导出适合结合律的乘法运算 (且有逆运算). 空字 e 为其单位元. 具有上面乘法运算的等价类的集合正好就是具有 n 个自由生成元 $a_1,\cdots,a_n$ 自由群 F_n, **即秩为 n 的自由群**.

例 一个拴着纱筒 (线轴) 的猫崽儿围着两个杆子按 "8" 字形各不同方向奔跑, 一边把线压在前面留下来的线上. 当猫崽儿经过两个杆子中心时, 它可能随意地按不同方向运动. 从中心点开始, 并在中心点结束, 猫所走过的路线显然可以解释为秩为 2 的自由群的元素.

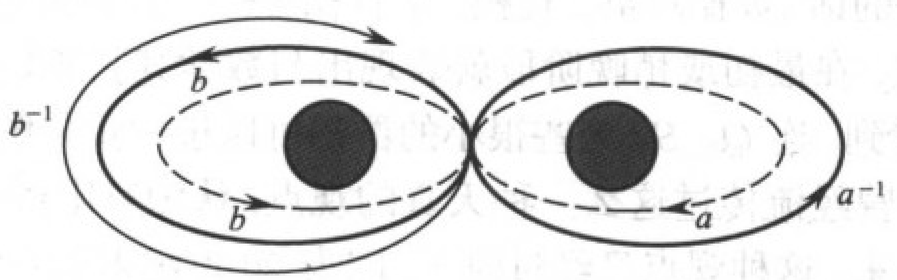


图 3

拉紧了的线, 即去除平凡的线圈 $aa^{-1},a^{-1}a,bb^{-1},b^{-1}b$ 所得的线路就是不可约字. 在图 3 中画出的 a 与 a^{-1}, b 与 b^{-1} 有间隔只是为了几何上的直观性. 我们的例子实现了 F_2 为双纽线 "同伦等价路线" (拓扑术语) 的类集合的形式. 从这一点来说, 自由群 F_5 是在注释第 3 章 §3 第 2 目的图 5 中分问题和解答部分所描述的蔓叶线的基本群.

第 2 章　群的结构

我们所研究的代数对象, 如果它们的特性能够用 (在某种意义上) 较初等的对象和运算语言来表达的话 (如循环群、直积、半直积等等), 会变得更加吸引人. 而这些对象本身 (比如群), 在最初或稍晚阶段就表现出与数学其它领域的紧密联系. 我们在第 1 章中已经看到, 连 Q_8, S_4 这些很小的群都可以进一步分解, 这些分解在很多方面都是有益的. 曾经流传过这么一种天真的观点, 认为有限群可以凭借凯莱定理就能够一一列举出来. 这种观点已经过时了, 因为 20 世纪末功率最大的计算机也没能证明出 "大得出奇的 M" 的存在, 这里 "大得出奇的 M" 指的是

$$|M| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

的单群. 这是人得出来的. 另一方面, 列举较小阶 $4096 = 2^{12}$ 的群 (精确到同构), 无论对机器还是对人来说,做起来都相当复杂.

在本章中, 注意力将集中在为数不多的群类, 熟悉它们, 对于每个数学工作者来说都是有益的.

§1 可解群与单群

1. 可解群　在第 1 章介绍的换位子群的概念带来重要的也是非常广泛的群类. 像以前一样, 令 G' 为群 G 的换位子群. 在 G' 中同样可以考虑换位子群 $(G')' = G''$, 它称为群 G 的**第二换位子群** (**第二导出子群**). 继续这样的过程, 我们可以定义第 k 个换位子群 $G^{(k)} = (G^{(k-1)})'$. 由第 1 章 §4 包含关系 (1), 我们有 $G^{(k)} \lhd G$, 从而当然也有 $G^{(k)} \lhd G^{(k-1)}$. 于是我们得到一个正规子群列 (导出列)

$$G \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq \cdots \trianglerighteq G^{(k)} \trianglerighteq G^{(k-1)} \trianglerighteq \cdots \tag{1}$$

其每个商因子 $G^{(k)}/G^{(k-1)}$ 都是交换群.

定义 一个群 G 称为**可解的**, 如果列 (1) 能够下降达到单位元群, 即存在一个最小指数 m, 使得 $G^{(m)}=e$. 此时 m 称为可解群 G 的**步长**.

显然, 任一交换群 (其中包括循环群) 的可解步长为 1. 此外, 在任一可解步长为 m 的可解群 G 中有一个 $\neq e$ 的交换正规子群, 它就是 $G^{(m-1)}$. 作为在第 1 章的例子中我们所看到的, $S_4'=A_4, A_4'=V_4, V_4'=e$, 于是交错群 A_4 的可解步长为 2, 而对称群 S_4 的可解步长为 3. 我们再看下列更一般的例子.

例 假设

$$T:=T(n,\mathfrak{K})=\{A=(a_{ij})\subset \mathrm{GL}(n,\mathfrak{K})|a_{ij}=0,\forall i>j\}$$

为系数属于任一域 $\mathfrak{K}$ 的上三角矩阵群. 直接验证知, $T^{(n+1)}=E$, 于是对任意 n, $T(n,\mathfrak{K})$ 是一个可解群. 顺便指出, T 的换位子群 $T'=\mathrm{UT}(n,\mathfrak{K})$ (主对角线元素为单位元的上三角矩阵群) 有比可解性更强的性质. 如果对于任一群 G, 令

$$G_1:=G, G_2=G', G_{k+1}=(G_k,G)=\langle (u,v)|u\in G_k, v\in G\rangle,$$

那么我们将得到群 G 的一个下中心列:

$$G=G_1\trianglerighteq G_2\trianglerighteq G_3\trianglerighteq\cdots\trianglerighteq G_k\trianglerighteq G_{k+1}\cdots. \tag{2}$$

一个群 G 称为 c 类幂零群, 如果 $G_c\neq e$, 但 $G_{c+1}=e$. 群 $\mathrm{UT}(n,\mathfrak{K})$ 是 n 类幂零群.

定理 1 假设 G 是一个群, K 是 G 的一个正规子群. 则 G 为可解群的充分必要条件是 K 和 G/K 都可解.

证明 如果 $H\subset G$, 那么 $H'\subset G',\cdots,H^{(k)}\subset G^{(k)}$, 由此直接推得, 可解群 G 的任意子群为可解群.

现在设 K 为可解群 G 的一个正规子群且 $\overline{G}=G/K$ 为相应的商群. 自然同态 $\pi:G\to\overline{G}$ 带来 G' 到 $\overline{G}'$ 上的满同态 (因为, 显然 $\varphi((g_1,g_2))=(\varphi(g_1),\varphi(g_2))$, 对于任一同态 $\varphi:G\to\overline{G}$), 从而也有 $G^{(k)}$ 到 $\overline{G}^{(k)}$ 上的满同态. 由此可知 $\overline{G}$ 是可解的.

为了证明定理的反向命题, 我们用 π 代替 φ, 就得到

$$(\bar{g}_1,\bar{g}_2)=\overline{(g_1,g_2)}, \tag{3}$$

即 $(g_1K,g_2K)=(g_1,g_2)K$ (应当在形式上区分 G 中的换位子和 $\overline{G}$ 中的换位子). 令 s 为商群 $\overline{G}$ 的可解步长, t 为正规子群 K 的可解步长. 反复利用 (3) 式, 对任意 i 我们得到等式 $\overline{G^{(i)}}=(\overline{G})^i$. 特别地, $\overline{G^{(s)}}=(\overline{G})^{(s)}=\overline{e}=K$. 于是, 有包含关系 $G^{(s)}\subset K$, 由此得到 $G^{(s+t)}\subset K^{(t)}=e$, 即 G 为一个可解群. □

推论　假设 K_1, K_2 为任一群 G 的两个可解正规子群, 那么 K_1K_2 同样是 G 的一个可解正规子群.

证明　由第 1 章我们已经知道, K_1K_2 是 G 的一个正规子群. 进一步, 由同构定理知

$$K_1K_2/K_2 \cong K_1/(K_1 \cap K_2).$$

于是应用定理 1 即得. □

由已经证明的推论得到下列断言. 有限群 G 的所有可解正规子群的积 $F(G)$ 是 G 的一个最大可解正规子群, 而其商群 $G/F(G)$[①] 已经不包括可解正规子群.

可解群的产生归功于伽罗瓦 (Galois) 定理, 这一点我们在 [BA I] 中已经谈到. 群 S_4 和它的子群的可解性是 n 次 ($n \leqslant 4$) 方程根式可解的依据. 这个问题的更详细信息可以在第 5 章 §5 中看到.

2. 单群　存在 $\neq e$ 的群, 它等于它的换位子群, 从而, 它不是可解群. 而且, 我们现在将证明存在非交换群, 它根本没有非平凡 (即不等于 e 和 G) 的正规子群. 这样的群称之为**单群**.

引理　一个群 G 的任一正规子群 K 是 G 的某些共轭元素类集合的并.

证明　如果 $x \in K \lhd G$, 那么, 对所有 $g \in G, gxg^{-1} \in K$. 于是, 当 $x \in K$ 时, K 就包括了 x 所在的整个共轭元素类 x^G, 于是 $K = \bigcup_{i \in I} x_i^G$. □

定理 2　交错群 A_5 是一个单群.

证明　事实上, 在 A_5 中, 除单位置换 e, 有 15 个 2 阶元 $(i\ j)(k\ l), 20 = 2\begin{pmatrix}5\\3\end{pmatrix}$ 个 3 阶元 $(i\ j\ k)$ 和 $24 = 4!$ 个 5 阶元 $\begin{pmatrix}1 & i_1 & i_2 & i_3 & i_4\end{pmatrix}$. 所有 2 阶元互相共轭: 它们在 S_5 中共轭是显然的, 而因为元素 $(1\ 2)(3\ 4)$ 的稳定子群 (关于共轭作用) 包含一个奇置换 $(1\ 2)$, 所以它们的共轭可由偶置换来实现. 对于 3 阶元同样. 但 5 阶元在 S_5 中互相共轭, 而在 A_4 中被分解为以 $\begin{pmatrix}1 & 2 & 3 & 4 & 5\end{pmatrix}$ 和 $\begin{pmatrix}1 & 2 & 3 & 5 & 4\end{pmatrix}$ 为代表元的两个互相共轭类. 事实上, $\begin{pmatrix}4 & 5\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4 & 5\end{pmatrix}\begin{pmatrix}4 & 5\end{pmatrix}^{-1} = \begin{pmatrix}1 & 2 & 3 & 5 & 4\end{pmatrix}$, 而 $\begin{pmatrix}1 & 2 & 3 & 4 & 5\end{pmatrix}$ 在 A_5 中的中心化子 (即稳定子群) 是由这 5 个元生成的循环群. 于是我们得到下表

1	15	20	12	12
e	(1 2)(3 4)	(1 2 3)	(1 2 3 4 5)	(1 2 3 5 4)

下行为共轭类的代表元, 上行为共轭类的势. 现在假设 K 为 A_5 的一个正规子群. 由

①一般书上, 符号 $F(G)$ 表示最大幂零正规子群 —— 译者注.

引理

$$|K| = \delta_1 \cdot 1 + \delta_2 \cdot 15 + \delta_3 \cdot 20 + \delta_4 \cdot 12 + \delta_5 \cdot 12,$$

其中 $\delta_1 = 1$ (因为 $e \in K$), $\delta_i = 0$ 或 $\delta_i = 1$, 对于 $i = 2, 3, 4, 5$. 不难验证, 由 $|K|$ 整除 A_5 的阶 $|A_5| = 60$ (拉格朗日定理), 只有下列两种可能:

a) $\delta_2 = \delta_3 = \delta_4 = \delta_5 = 0$; K 为单位元群;

b) $\delta_2 = \delta_3 = \delta_4 = \delta_5 = 1$; $K = A_5$.

于是, 这就证明了 A_5 是一个单群. □

利用对 n 的归纳法可以证明 (参见习题 3), 当 $n \geqslant 5$ 时, 所有 A_n 都是单群. 由于可解群的子群都是可解群 (定理 1), 所以由定理 2 知, 在任何情况下, 对称群 $S_n (n \geqslant 5)$ 都是非可解的.

定理 3 *旋转群* SO(3) *是单群.*

证明 由第 1 章 §1 定理 1, 只需验证, 在满同态 $\Phi : \mathrm{SU}(2) \to \mathrm{SO}(3)$ 下, 群 SU(2) 的包含同态核 $\{\pm E\}$ 且不等于核的任一正规子群 K 等于 SU(2). 第 1 章 §1 关系 (5) 可以重新解释为: 群 SU(2) 的每个共轭类中包含对角矩阵 $d_\varphi = b_2\varphi = \mathrm{diag}\{e^{i\varphi}, e^{-i\varphi}\}$. 因为由引理, K 是群 SU(2) 中某些共轭类的并, 所以不失一般性, 我们可以认为 $d_\varphi \in K$, 对于某个满足 $\sin\varphi \neq 0$ 的 $\varphi > 0$.

在 K 中也应该包括任意换位子

$$(d_\varphi, g) = d_\varphi\left(g d_\varphi^{-1} g^{-1}\right) = \begin{pmatrix} e^{i\varphi} & 0 \\ 0 & e^{-i\varphi} \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \begin{pmatrix} e^{-i\varphi} & 0 \\ 0 & e^{i\varphi} \end{pmatrix} \begin{pmatrix} \overline{\alpha} & -\beta \\ \overline{\beta} & \alpha \end{pmatrix}$$
$$= \begin{pmatrix} |\alpha|^2 + |\beta|^2 e^{i2\varphi} & \\ & |\alpha|^2 + |\beta|^2 e^{-i2\varphi} \end{pmatrix},$$

其中 $|\alpha|^2 + |\beta|^2 = 1$ (见第 1 章 §1 第 1 目 (3)). 于是, 对于矩阵 (d_φ, g) 的迹, 我们有表达式

$$\mathrm{tr}(d_\varphi, g) = 2|\alpha|^2 + |\beta|^2\left(e^{i2\varphi} + e^{-i2\varphi}\right) = 2(1 - 2|\beta|^2 \sin^2\varphi).$$

这里 $|\beta|$ 取区间 $[0,1]$ 中任何值且 $\sin\varphi \neq 0$. 再次由第 1 章 §1 (5), 存在酉矩阵 $h \in \mathrm{SU}(2)$ 满足 $h[d_\varphi, g]h^{-1} = d_\psi = \mathrm{diag}\{e^{i\psi}, e^{-i\psi}\}$, 且 $d_\psi \in K$. 因为 $e^{i\psi}, e^{-i\psi}$ 都是矩阵 (d_φ, g) 的特征方程

$$\lambda^2 + (4|\beta|^2 \sin^2\varphi - 2)\lambda + 1 = 0$$

的根, 所以, $|\beta|$ 不得不跑遍由 0 到 1 的值, 从而我们得到 ψ 在区间上的任意点. 于是, 在 K 中包含任意元 d_ψ 和由参数 ψ 确定的共轭类, 这里 $0 \leqslant \psi \leqslant 2\varphi$. 因为对于

任意的 $\sigma > 0$, 可以找到自然数 n, 使其满足条件 $0 < \psi := \delta/n \leqslant 2\varphi$, 可以断言, K 包含事先给的元 $d_\sigma = d_\psi^n$. □

定理 4 设 F 是一个域且 F 的元素的个数 $|F| > 3$. 则 F 上的特殊射影线性群 $\mathrm{PSL}(2,F)$ 是一个单群.

证明 1) 我们选出一些子群和元:

$$U = \left\{ u(\alpha) = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \middle| \alpha \in F \right\},$$

$$\overline{U} = \left\{ \overline{u}(\alpha) = \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix} \middle| \alpha \in F \right\},$$

$$D = \left\{ d(\lambda) = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \middle| \lambda \in F^* \right\};$$

$$B = DU = UD = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{pmatrix} \right\}$$

是一个标准的**博雷尔子群**. 我们看到

$$d(\lambda) = u(\lambda - 1)\overline{u}(1)u(\lambda^{-1} - 1)\overline{u}(-\lambda),$$

于是博雷尔子群由**幂单子群** U 和 $\overline{U}$ 生成. 我们再选取元素

$$w = u(1)\overline{u}(-1)u(1) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

2) 群 $G = \mathrm{SL}(2,F)$ 有分解

$$G = B \cup BwB, \quad B \cap BwB = \varnothing. \tag{4}$$

为了确信这一点, 我们来考虑 G 在列上的左作用. 列为 $e^1[1,0]$ 的迷向群显然等于 U. 轨道 Be^1 由所有列 $[\lambda,0], \lambda \neq 0$, 组成. 另一方面, $we^1 = [0,-1]$, 因此, 轨道 Bwe^1 由所有第二个分量不等于零的列 $[\beta, \lambda^{-1}]$ 组成. 因为这两个列布满了列 Ge^1, 由此得到 $B \cup BwB = G$, 因为迷向群 U 含于 B.

分解式 (4) 称为布吕阿 (Bruhat) 分解. 该分解式可进一步深入, 我们不再讨论.

3) 博雷尔子群 B 是 G 的极大子群.

事实上, 由分解式 (4) 我们看到, 任意不包含在 B 的元 $h \in H$, 一定包含在 BwB 中, 即 $h = b_1 w b_2$, 于是 $w \in H$, 由此得到 $H = G$.

4) 如果 $|F| \geqslant 4$, 那么 $G = \mathrm{SL}(2,F) = G'$.

取 $0 \neq \lambda \in F, \lambda^2 \neq 1$, 这在 $|F| > 3$ 时是可能的. 那么由交换关系

$$d(\lambda)u(\alpha)d(\lambda)^{-1}u(\alpha)^{-1} = u(\alpha(\lambda^2 - 1))$$

得到 $B' = U$ 且 $G' \supset U$, 而因为 $G' \lhd G$, 我们有包含关系 $G' \supset wUw^{-1} = \overline{U}$. 但是, 由 1) 和 2), 我们知道 U 和 $\overline{U}$ 生成 G. 于是 $G' = G$.

5) 在 $|F| \geqslant 4$ 时, 群 $\mathrm{PSL}(2, F) = \mathrm{SL}(2, F)/Z$ 是单群 (这里 $Z = \{\pm E\}$ 为中心).

运用容易验证的等式

$$\bigcap_{x \in G} xBx^{-1} = Z.$$

我们需要证明, 如果 $H \lhd G = \mathrm{SL}(2, F)$, 那么要么 $H \subset Z$ 要么 $H \supset G'$. 由 B 的极大性 (见 3)), 我们有 $HB = B$ 或 $HB = G$. 如果 $HB = B$, 那么 $H \subset B$. 因为 $H \lhd G$, 所以 $H = xHx^{-1} \subset xBx^{-1}, \forall x \in G$, 即 $H \subset Z$.

另一方面,

$$HB = G \Longrightarrow w = hb, h \in H, \quad b \in B.$$

于是由 $H \lhd G$ 有

$$\overline{U} = wUw^{-1} = hbUb^{-1}h^{-1} = hUh^{-1} \subset HU.$$

因为 $U \subset HU$, 且 $U, \overline{U}$ 生成 G, 所以 $HU = G$. 从而

$$G/H = HU/H \cong U/(U \cap H)$$

是一个交换群, 由此得到 $G' \subset H$. 因此 $\mathrm{PSL}(2, F)$ 是一个单群. □

定理 4 曾被伽罗瓦首次用其它方式证明. 由定理 2 ~ 4 可以看到, 在单群类中包含有重要应用的群, 有限群和无限群. 可能觉得奇怪, 稍为合理地描写一下所有存在的单群就需要几百页.

习 题

1. 子群链

$$e = G_0 \subset G_1 \subset \cdots \subset G_n \subset G_{n+1} = G, \tag{*}$$

其中 $G_{i-1} \lhd G_i, 1 \leqslant i \leqslant n+1$, 称为群 G 的一个正规列. 一个下降的群列

$$G = G_0 \supset G_1 \supset \cdots \supset G_n \supset G_{n+1} = e,$$

其中 $G_{i+1} \lhd G_i$, 同样也称为正规列.

如果列 (*) 中所有成员互不相同且 $G_{i-1} \lhd H \lhd G_i \Longrightarrow H = G_{i-1}$ 或 $H = G_i$, 对所有 i, 那么就称这个正规列为 G 的一个合成列. 在这种情况下, $F_i = G_i/G_{i-1}$ 称为 G 的一个合成因子.

试证:

1) 有限群的任一个正规列可以加细为一个合成列, 即插入一些补充项, 直到为合成列为止;

2) 商因子 F_i 是单群 (或素数阶循环群);

3) 一个群 G 是可解的当且仅当它的所有合成因子是素数阶循环群.

我们不予证明地提到若尔当–赫尔德 (Jordan-Hölder) 定理, 利用该定理我们知道群 G 的一组合成因子精确到同构以及随之它的阶是不依赖于合成列的选取的.

2. 证明, 任一有限 p–群是可解群.

3. 按照下列提要来证明交错群 A_n, 当 $n \geqslant 5$ 时, 是单群.

a) 设 $K \lhd A_n$ 且 $K \neq e$, 则 K 中有一个置换 $\pi \neq e$. 假设 π 保持 $\Omega = \{1, 2, \cdots, n\}$ 中不动元素最大可能的个数为 m. 如果 $m = n-3$, 则 $\pi = (ijk)$, 于是 $K = A_n$ (参见 [BA I] 第 4 章, §2, 练习 11), 于是可以认为 $m < n-3$.

b) 如果 $\pi = (1\,2\,3\cdots)\cdots$ 为 π 的不相交循环的分解, 那么 π 的偶置换性及条件 $m < n-3$ 导致了 $m < n-5$. 还有可能 $\pi = (1\ 2)(3\ 4)\cdots$ 为长为 2 不相交循环组成.

c) 在任何情况下, 考虑换位子 $(\pi, \sigma) = \pi\sigma\pi^{-1}\sigma^{-1} \neq e$, 其中 $\sigma = (3\,4\,5)$, 验证, 它保持不动点的个数大于 m. 这与 m 的选取矛盾, 于是断言成立.

4. 证明, 交错群 A_5 不包含 15 阶和 20 阶子群.

§2 西罗 (Sylow) 定理

我们已经看到这样的事实, 在一个阶为 $|G|$ 的有限群 G 中可能没有 d 阶子群, 这里 d 整除 $|G|$. $G = A_4, d = 6$ 就是这样的一个极小例子.

因为在非交换单群中没有指数为 2 的子群 (指数为 2 的子群是正规的), 所以由 §1 的定理 2, 在 60 阶的交错群 A_5 中没有 30 阶的子群 (也参见 §1 习题 4). 在这种背景下, 125 年前挪威数学家西罗创立的一般规律显然非常出色. 这些规律性与作为子群身份包含在群 G 中的 p–群有关 (p–群在第 1 章 §3 中我们已经见过). A. 柯西发现, 在被 p 整除其阶的交换群中存在 p 阶元.

设 $|G| = p^n m$, 这里 p 为一个素数, 而 m 是一个与 p 互素的整数. 阶为 p^n 的子群 $P \subset G$ (如果存在) 将被称为群 G 的一个*西罗 p–子群*. 正如第 1 章 §3 中所讲的, 用 $N(P)$ 表示子群 P 在 G 中的正规化子.

定理 1 (第一西罗定理)　*西罗 p–子群存在.*

定理 2 (第二西罗定理)　*假设 P 和 P_1 是群 G 的两个西罗 p–子群, 那么存在元 $a \in G$, 使得 $P_1 = a^{-1}Pa^{-1}$. 换句话说, 所有西罗 p–子群互相共轭.*

定理 3 (第三西罗定理)　*假设 N_p 为群 G 中西罗 p–子群的个数. 那么 $N_p = (G : N(P))$ 且 $N_p \equiv 1 (\operatorname{mod} p)$.*

定理 1 至定理 3 的证明是第 1 章 §3 中所叙述的一般方法和思路的例证. 我们先证定理 2.

定理 2 的证明. 假设在群 G 中存在 西罗 p–子群且令 P 是它的一个 西罗 p–子群. 再令 P_1 是群 G 的任一个 p–子群, 不一定是西罗子群. 让 P_1 左平移地作用在 G 关于 P 的左陪集集合 $G/P = \bigcup\limits_i g_iP$ 上 (限制 G 的作用在 G/P 上的描写见第 1 章 §3). 由第 1 章的结果, 任一 P_1 轨道的长整除 $|P_1| = p^k, k \leqslant n$. 于是

$$m = \frac{p^n m}{p^n} = \frac{|G|}{|P|} = |G/P| = p^{k_1} + p^{k_2} + \cdots,$$

其中 $p^{k_1}, p^{k_2}, \cdots$ 是轨道长. 因为 g.c.d $(m, p) = 1$, 所以至少有一个轨道的长 $p^{k_i} = 1$, 即

$$P_1 \cdot aP = aP \tag{1}$$

对于某个元 $a = g_i \in G$ (这类似于第 1 章 §3 定理 2 的证明). 将等式 (1) 改写为 $P_1 \cdot aPa^{-1} = aPa^{-1}$, 那么我们将得到包含关系

$$P_1 \subset aPa^{-1} \tag{2}$$

(因为 aPa^{-1} 是群). 特别地, 如果 P_1 是群 G 的西罗 p–子群, 那么由 $|P_1| = |P|$ 以及 (2) 式, 我们得到 $P_1 = aPa^{-1}$. □

定理 1 和 3 的证明 定理 1 可以解释为定理 3 的推论, 这因为 $N_p \equiv 1 (\bmod p)$, 而 $N_p \neq 0$ 的充分必要条件是 $S \neq \varnothing$, 这里 S 为群 G 的所有西罗 p–子群的集合. 现在来证定理 3. 等式 $N_p = (G : N(P))$ 由西罗 p–子群的共轭性 (定理 2) 以及第 1 章 §3 中关于轨道 H^G 的长的一般结论直接推得. 对于 $N_p \equiv 1 (\bmod p)$, 我们来考虑几个更一般的情形. 假设 $|G| = p^s t$, 这里 $s \leqslant n, t$ 可以被 p 整除且令 $N_p(s)$ 为 G 中所有阶为 p^s 的子群的个数. 原来也有等式 $N_p(s) \equiv 1 (\bmod p)$; 特别地, G 包含任意阶为 p^s 的子群且 $N_p(n) = N_p$.

我们用下列方法来证明上面这一断言. 根据第 1 章 §3 第 1 目最后的注, 我们知道, 群 G 在自身上的左平移作用诱导一个 G 在集合

$$\Omega = \{M \subset G \mid |M| = p^s\}$$

上的作用, 这里 Ω 是所有 p^s–元子集 $\{g_1, \cdots, g_{p^s}\}$ 的集合. 我们知道, $g \cdot \{g_1, \cdots, g_{p^s}\} = \{gg_1, \cdots, gg_{p^s}\}$. 集合 Ω 有 G–轨道分解: $\Omega = \bigcup\limits_i \Omega_i$, 于是

$$|\Omega| = \sum_i |\Omega_i|, \ |\Omega_i| = (G : G_i),$$

这里 $G_i = \{g \in G | gM_i = M_i\}$ 为某个代表元 $M_i \in \Omega_i$ 的稳定子群.

因为 $G_iM_i = M_i$, 那么 $M_i = \bigcup_{j=1}^{\nu_i} G_i g_{ij}$ 是 G 关于 G_i 的某些右陪集的并. 因此 $p^s = |M_i| = \nu_i |G_i|$, 从而 $|G_i| = p^{s_i} \leqslant p^s$. 如果 $|G_i| < p^s$, 那么 $|\Omega_i| = p^{s-s_i} t \equiv$

$0(\mathrm{mod}\, pt)$; $|G_i| = p^s$ 与 $|\Omega_i| = t$ 是等价的. 于是我们得到

$$\binom{|G|}{p^s} = |\Omega| \equiv \sum_{|\Omega_i|=t} |\Omega_i| (\mathrm{mod}\, pt). \tag{3}$$

根据上面所说的, $|\Omega_i| = t \Longrightarrow |G_i| = p^s \Longrightarrow M_i = G_i a_i$ (其中 $a_i = g_{ij}$ 为 G 的某一个元), 于是 $a_i^{-1} M_i = a_i^{-1} G_i a_i = P_i$ 是 p^s 阶子群. 这表明, 轨道 Ω_i 是群 G 关于 P_i 的一些左陪集 gP_i 的集合.

反之, 群 G 的每个阶为 p^s 的子群 H 属于轨道 $\Omega' = \{gH | g \in G\}$, 其长为 t. 阶为 p^s 的不同的子群 H_i 属于不同的轨道 Ω'_i, 这因为由 $H_i = gH_j$ 推出 $e = gh_j$, 于是 $g = h_j^{-1} \in H_j$, 从而 $H_i = H_j$. 因此, 在阶为 p^s 的子群与长为 t 的轨道 Ω_i 之间存在一一对应. 于是等式 (3) 可改写为

$$\binom{|G|}{p^s} \equiv \sum_{|\Omega_i|=t} |\Omega_i| \equiv tN_p(s) (\mathrm{mod}\, pt), \tag{4}$$

这里如果强调 $N_p(s)$ 与 G 的关系, 也可以写为 $N_p(s, G)$.

到现在为止, 群 G 的特性还没有用上. 如果 G 是阶为 $p^s t$ 的一个循环群, 那么 $N_p(s, G) = 1$ (第 1 章 §2 定理 3), 从而

$$\binom{|G|}{p^s} \equiv t \cdot 1 (\mathrm{mod}\, pt). \tag{5}$$

因为等式 (4) 和 (5) 左边相等, 所以我们有

$$t \equiv tN_p(s) (\mathrm{mod}\, pt),$$

由此得到了 $N_p(s) \equiv 1 (\mathrm{mod}\, p)$. □

虽然实际上的证明比要求的要多, 但我们不打算继续运用它, 有兴趣的读者可以参看一些专业文章.

例 假设 $G = \mathrm{SL}(2, Z_p)$ 为 p 元域 Z_p 上行列式为 1 的所有 2×2 矩阵构成的群. 由完全线性群 $\mathrm{GL}(2, Z_p)$ 关于 $\mathrm{SL}(2, Z_p)$ 的左陪集分解式

$$\mathrm{GL}(2, Z_p) = \bigcup_{i=1}^{p-1} \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \mathrm{SL}(2, Z_p)$$

推得

$$|\mathrm{GL}(2, Z_p)| = (p-1)|\mathrm{SL}(2, Z_p)|. \tag{6}$$

将 $\mathrm{GL}(2, Z_p)$ 看成域 Z_p 上的二维向量空间 V 的自同构群, 容易算出阶 $|\mathrm{GL}(2, Z_p)|$. 事实上, $\mathrm{GL}(2, Z_p)$ 作用在一组基 $\{\mathbf{v}_1, \mathbf{v}_2\}$ 上. 任一个非零向量 $\mathbf{f}_1 \in V$ 可以作为 $\mathbf{v}_1$

的像 (这样的 $\mathbf{f}_1$ 有 p^2-1 个), 而在 $\mathbf{f}_1$ 选取之后, $\mathbf{v}_2$ 的像可以是 $V\backslash\langle\mathbf{f}_1\rangle$ 中的任一个向量 (这样的 $\mathbf{f}_2$ 有 p^2-p 个). 于是 $|\mathrm{GL}(2,Z_p)|=(p^2-1)(p^2-p)$, 从而由 (6) 推得

$$|\mathrm{SL}(2,Z_p)|=p(p^2-1).$$

我们一下子就找到群 $\mathrm{SL}(2,Z_p)$ 至少有 2 个西罗 p–子群:

$$P=\left\{\begin{pmatrix}1&\alpha\\0&1\end{pmatrix}\middle|\,\alpha\in Z_p\right\},\quad \overline{P}=\left\{\begin{pmatrix}1&0\\\alpha&1\end{pmatrix}\middle|\,\alpha\in Z_p\right\}.$$

根据定理 3, 我们有

$$N_p=(G:N(P))=1+kp>1,$$

而因为

$$\begin{pmatrix}\lambda&0\\0&\lambda^{-1}\end{pmatrix}\begin{pmatrix}1&\alpha\\0&1\end{pmatrix}\begin{pmatrix}\lambda^{-1}&0\\0&\lambda\end{pmatrix}=\begin{pmatrix}1&\lambda^2\alpha\\0&1\end{pmatrix}$$

从而正规化子 $N(P)$ 包括下列阶为 $p(p-1)$ 的子群

$$H=\left\{\begin{pmatrix}\lambda&\alpha\\0&\lambda^{-1}\end{pmatrix}\middle|\,\alpha,\lambda\in Z_p,\lambda\neq 0\right\},$$

于是只有一种可能

$$N(P)=H,N_p=1+p.$$

在群

$$\mathrm{SL}(2,Z_2)=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&1\\1&0\end{pmatrix},\begin{pmatrix}0&1\\1&1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}1&0\\1&1\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}\right\}$$

与对称群 S_3 之间直接建立一个同构

$$(1\ 2\ 3)\mapsto\begin{pmatrix}1&1\\1&0\end{pmatrix},(1\ 2)\mapsto\begin{pmatrix}0&1\\1&0\end{pmatrix}$$

(这两个群有相同的生成元和对应关系). 当 $p>2$ 时, 群 $G=\mathrm{SL}(2,Z_p)$ 有中心 $Z(G)=\{\pm E\}$, 其阶为 2. 商群 $\mathrm{PSL}(2,Z_p)=G/Z(G)$, 正如 [BA II] 中所说, 被自然地称为特殊射影线性群 (它是射影直线

$$Z_p\mathbb{P}^1=\mathbb{P}(V)=\{0,1,\cdots,p-1\}\bigcup\{\infty\}$$

的变换群), 自伽罗瓦时代起, 该群在代数中就扮演着重要的角色. 事实上, 在 $p>3$ 时, 群 $\mathrm{PSL}(2,Z_p)$ 是一个单群, 而这与 A_n 一样, 是有限单群最早的例子之一.

我们再来看一般情况, 得到西罗定理的一个有益的加细.

定理 4　下列断言正确:

i) 群 G 的西罗 p–子群 P 在 G 中正规当且仅当 $N_p = 1$;

ii) 阶为 $|G| = p_1^{n_1} \cdots p_k^{n_k}$ 的群 G 是其西罗 p_i–子群 $P_1, \cdots, P_k$ 的直积当且仅当所有这些西罗子群在 G 中是正规的.

证明　i) 对于群 G 的阶 $|G|$ 的每个给定的素因子 p, 由第二西罗定理知, 所有西罗 p–子群是互相共轭的, 于是, 如果 P 是 G 的一个西罗p–子群, 那么

$$N_p = 1 \Longleftrightarrow xPx^{-1} = P, \forall x \in G \Longleftrightarrow P \lhd G.$$

ii) 如果 $G = P_1 \times \cdots \times P_k$ 是它的所有西罗子群的直积, 那么 P_i 作为 G 的任意直因子当然是正规的, 即 $P_i \lhd G$. 也就是说, 正规性条件是肯定的.

现在假设 $P_i \lhd G, 1 \leqslant i \leqslant k$, 那么 $N_{p_i} = 1$, 于是, 首先有

$$x \in P_i \bigcap P_j, i \neq j \Longrightarrow x^{p_i^s} = e, x^{p_j^t} = e \Longrightarrow x = e.$$

这表明 $P_i \bigcap P_j = e$, 由此知, 对于任意 $x_i \in P_i, x_j \in P_j$, 我们有

$$(x_i, x_j) = \begin{cases} \left(x_i x_j x_i^{-1}\right) x_j^{-1} = x_j' x_j^{-1} \in P_j \\ x_i \left(x_j x_i^{-1} x_j^{-1}\right) = x_i x_i' \in P_i \end{cases} \Longrightarrow (x_i, x_j) = e,$$

也就是说, 元素 x_i 与 x_j 相乘可交换.

我们再看一下, 假设群 G 的单位元 e 写为 $e = y_1 y_2 \cdots y_k$, 这里 $y_i \in P_i$ 是阶为 $a_i = p_i^{b_i}$ 的元. 那么令 $a = \prod\limits_{i \neq j} a_i$ 且利用元素 $y_1, \cdots, y_k$ 相乘的可换性, 我们得到

$$e = (y_1 y_2 \cdots y_k)^a = y_1^a y_2^a \cdots y_k^a = y_j^a.$$

但是因为 a 与 a_j 互素, 所以由 $y_j^{a_j} = y_j^a = e \Longrightarrow y_j = e$. 这对任意的 j 成立. 于是由等式 $e = y_1 y_2 \cdots y_k$ 必然推得 $y_1 = y_2 = \cdots = y_k = e$.

另一方面, G 中阶为 $r = r_1 r_2 \cdots r_k$ 的每个元 x, 这里 $r_i = p_i^{s_i}$, 可以写为形式

$$x = x_1 x_2 \cdots x_k, \quad |\langle x_i \rangle| = r_i, \quad 1 \leqslant i \leqslant k. \tag{7}$$

这只需令 $x_i = x^{t_i r_i'}$, 其中指数由下列条件定义

$$r_i' = \frac{r}{r_i}, \quad 1 = \sum_{i=1}^{k} t_i r_i'.$$

如果现在 $x = x_1' x_2' \cdots x_k'$ 为 x 的另一个 p_i–元积的形式, 那么由于 x_i, x_i' 与具有不同下标的元相乘可换, 所以

$$e = (x_1' x_2' \cdots x_k')(x_1 x_2 \cdots x_k)^{-1} = x_1' x_1^{-1} \cdot x_2' x_2^{-1} \cdots x_k' x_k^{-1}.$$

但由上面我们刚刚证明的知道, $x_1'x_1^{-1}=x_2'x_2^{-1}=\cdots=x_k'x_k^{-1}=e$, 即 $x_1'=x_1,x_2'=x_2,\cdots,x_k'=x_k$.

这表明, G 的每一个元可以写成而且可以唯一地写成 (7) 的形式, 因此 (参见 §2) $G=P_1\times\cdots\times P_k$. □

注 一个群 G 的正规西罗 p–子群是 G 的一个**特征子群**, 也就是说, 在任意自同构 $\varphi\in\mathrm{Aut}(G)$ 作用下不变. 事实上, 因为 $|\varphi(P)|=P$, 所以 $\varphi(P)$ 也是 G 的一个西罗 p–子群, 于是如果 $N_p=1$, 则 $\varphi(P)=P$. 同样值得指出的是, 在不同于有限群的代数结构中西罗子群的类似也得到了研究.

习 题

1. 在 A_5 中找出西罗 5–子群的个数.

2. 验证: Z_3 上的矩阵

$$\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\pm\begin{pmatrix}1&-1\\-1&-1\end{pmatrix},\pm\begin{pmatrix}-1&-1\\-1&1\end{pmatrix},\pm\begin{pmatrix}0&1\\-1&0\end{pmatrix}$$

的集合 P 构成一个同构于四元数群 Q_8 的群, 且 P 是 $\mathrm{SL}(2,Z_3)$ 的一个西罗 2–子群. 并证明 $P\lhd\mathrm{SL}(2,Z_3)$.

3. 证明, 群 S_4 与 $\mathrm{SL}(2,Z_3)$ 不同构. $\mathrm{PSL}(2,Z_3)$ 与 A_4 同构吗?

4. 证明, 任一阶为 $pq(p<q$都为素数) 的群 G 要么是循环群, 要么是具有正规西罗 q–子群的非交换群, 而且后者成立的充分必要条件是 $p|(q-1)$. 特别地, 所有 15 阶群是循环群.

5. 通过直接计算西罗 p–子群在对称群 S_p 中的个数 N_p 来重新验证 (见 [BA I] 第 6 章 §1 例 3) 等式 $(p-1)!+1\equiv 0(\mathrm{mod}\,p)$.

6. 证明, 阶 $|G|\leqslant 30$ 的群不是单群.

§3 有限生成交换群

这一节的叙述较少依赖于本章的其它内容.

1. 例子和初步结果 正如我们不止一次地提到, 交换群有时为了方便可以写为加法运算, 用 + 表示该运算. 于是, 如果 $(A,+)$ 是一个加法交换群, 那么:

1) $a+a'=a'+a$, 对于任意元 $a,a'\in A$;

2) $na:=\underbrace{a+a+\cdots+a}_{n}$, 对于任意 $n>0$ 且 $n\in\mathbb{Z}$;

3) $0\cdot a=0$ (左边 $0\in\mathbb{Z}$, 右边 0 为群的单位元);

4) $(-n)a=\underbrace{(-a)+(-a)+\cdots+(-a)}_{n}$, 对任意 $n>0,n\in\mathbb{Z}$.

由上面这些性质推得

$$m(na) = (mn)a, \quad (m+n)a = ma + na, \quad n(a+a') = na + na'.$$

于是, 对于任意一组元 $a_1, \cdots, a_m \in A$, 我们可以讨论整系数组合

$$n_1a_1 + n_2a_2 + \cdots + n_ma_m \in A, \text{ 其中 } n_i \in \mathbb{Z}.$$

定义　*加法交换群 A 的元素组 $a_1, \cdots, a_m$ 称为群 A 的生成系, 如果*

$$\{n_1a_1 + \cdots + n_ma_m | n_i \in \mathbb{Z}\} = A,$$

也就是说, 每个元 $a' \in A$ 可以写为 (可能有多种方式) 形式: $a' = n_1a_1 + \cdots + n_ma_m$. 在这种情况下, 我们写

$$A = \langle a_1, a_2, \cdots, a_m \rangle.$$

例 1　通常单位元 1 是 $(\mathbb{Z}, +)$ 的一个生成元; -1 也是一个生成元, 但 $n \neq \pm 1$ 不是它的生成元.

例 2　整数向量 (向量带整数坐标) 的交换群 $\mathbb{Z}^n$ 在坐标空间 $\mathbb{Q}^n$ 中有生成系

$$\varepsilon_1 = (1, 0, \cdots, 0), \quad \varepsilon_2 = (0, 1, \cdots, 0), \quad \cdots, \quad \varepsilon_n = (0, 0, \cdots, 1).$$

例 3　在群 $\mathbb{Z}^2$ 中可以选择其它生成系, 例如,

$$b_1 = (1, 1), \quad b_2 = (1, -1), \quad b_3 = (4, 1).$$

因为 $\varepsilon_1 = 3b_1 + 2b_2 - b_3, \varepsilon_2 = -2b_1 - 2b_2 + b_3$, 所以它们确实生成群 $\mathbb{Z}^2$. 同时集合 $\{b_1, b_2, b_3\}$ 中的任两个元都不是 $\mathbb{Z}^2$ 的生成系. 试验证这一点.

不难说出没有任何有限生成系的群. 例如,

$$\mathbb{R}^{(+)} = (\mathbb{R}, +) \text{ 和 } U = \{\alpha \in \mathbb{C} | |\alpha| = 1\} \text{ (} U \text{ 的运算为乘法)}$$

就是这样的群. 实际上, 这些群都是不可数的, 而具有有限生成系的群都是可数的. 还有其它例子: $\mathbb{Q}^{(+)}$ 或 $\mathbb{Q}^*$ (不难验证).

命题 1　*有限多个循环群 A_i 的直和 $A = A_1 \oplus \cdots \oplus A_n$ 是具有有限生成系的群.*

证明　事实上, 如果 $A_i = \langle a_i \rangle$, 那么元素,

$$(a_1, 0, \cdots, 0), (0, a_2, \cdots, 0), \cdots, (0, 0, \cdots, a_n)$$

就是群 A 的生成元. □

命题 2 两个有限循环群 C_m 和 C_n (其中 m, n 互素) 的直和 $A = C_m \oplus C_n$ 是阶为 mn 的循环群.

证明 见 [BA I] 第 4 章 §2 习题 3. □

于是, 我们有断言

$$\text{如果 g.c.d}(m, n) = 1 \Longrightarrow C_m \oplus C_n \cong C_{mn}. \tag{1}$$

我们看到, 具有有限多个生成元的交换群非常之多 (按各自的性质, 五花八门). 它们值得被详细地研究, 因为至少它们以自然的方式出现在几何、拓扑和同调代数中. 也值得补充说一下, 如果 G 是任意一个有限生成群 (这是一个广泛的群类), 那么由第 1 章 §4 定理 5 知, 群 G 关于其换位子群 G' 的商群也是具有有限多个生成元的交换群.

2. 无挠交换群 按照定义, 群 A 称为**无挠群**, 如果它没有有限阶的非零元, 即如果 $na = 0, n \neq 0 \Longrightarrow a = 0$. 这种群与向量空间非常相似, 这一点将在下面看到.

定义 元素系 $a_1, \cdots, a_k \in A$ 称为无关的, 如果由等式 $n_1a_1 + \cdots + n_ka_k = 0$, 其中 $n_i \in \mathbb{Z}$, 总推得

$$n_1 = \cdots = n_k = 0.$$

元素系 $a_1, \cdots, a_n \in A$ 称为是一个**基**, 如果满足下列两个条件:

1) 它是无关的;

2) 它是群 A 的生成元系.

引理 1 如果 $A = \langle a_1, \cdots, a_m \rangle$, 且元素 $b_1, \cdots, b_n \in A$ 是无关的系, 那么 $n \leqslant m$.

证明 用 $a_1, \cdots, a_m$ 表示 b_i:

$$b_i = \sum_{j=1}^{m} \beta_{ij} a_j, \quad \beta_{ij} \in \mathbb{Z}.$$

我们来看整数行向量 $B_i = (\beta_{i1}, \cdots, \beta_{im}) \in \mathbb{Q}^m$ ($\mathbb{Q}$ 上的坐标向量空间). 假设结论不成立, 即 $n > m$, 那么我们可以断定 $\{B_1, \cdots, B_n\}$ 是线性相关的. 于是可以找到不全为零的 $r_i \in \mathbb{Q}$ 满足

$$r_1B_1 + r_2B_2 + \cdots + r_nB_n = 0. \tag{2}$$

令 d 为数 r_i 的有理公分母: $r_i = s_i/d, s_i \in \mathbb{Z}$, 用 d 乘等式 (2) 的两边, 得到关系式

$$s_1B_1 + s_2B_2 + \cdots + s_nB_n = 0$$

其所有系数为整数. 将该向量方程分别写出来, 就得下列线性方程组

$$s_1\beta_{1j} + s_2\beta_{2j} + \cdots + s_n\beta_{nj} = 0, \quad 1 \leqslant j \leqslant m.$$

于是得到

$$\sum_{i=1}^{n} s_i b_i = \sum_{i=1}^{n} s_i \left(\sum_{j=1}^{m} \beta_{ij} a_j\right) = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} s_i \beta_{ij}\right) a_j = 0.$$

这与 $b_1, \cdots, b_n$ 无关矛盾. □

定理 1 下列断言正确:

1) 任一有限生成的无挠交换群 A 有基;

2) A 的所有基等势 (即由相同个数的元组成).

证明 1) 一般而言, 可以减少生成元系中生成元的个数, 但也许还没有达到无关. 设 $\{a_1, \cdots, a_m\}$ 为群 A 的某个生成元系. 形如 $s_1 a_1 + \cdots + s_m a_m = 0$ 的表达式自然地称为 $a_1, \cdots, a_m$ 上的一个关系. 数 $\min\limits_i |s_i|$ 将称为这个关系的高, 而 $a_1, \cdots, a_m$ 上高为极小的关系称为极小关系. 这样的关系总是存在的, 因为高是一个自然数. 另一方面, 极小关系不一定是唯一的. 证明分解为下列一系列简单的断言.

a) 如果 $s_1 a_1 + \cdots + s_m a_m = 0$ 为一个极小关系, 那么 $\text{g.c.d}(s_1, \cdots, s_m) = 1$.

事实上, 如果 $s_i = d s_i', 1 \leqslant i \leqslant m$, 那么

$$d(s_1' a_1 + \cdots + s_m' a_m) = 0 \Longrightarrow s_1' a_1 + \cdots + s_m' a_m = 0,$$

这因为 A 是无挠群. 如果 $d > 1$, 那么我们就得到一个更小的高, 与已选择的极小性矛盾.

b) 如果 $s_1 a_1 + \cdots + s_m a_m = 0$ 是高为 1 的关系, 且 $|s_k| = 1$, 那么 $m-1$ 个元的集合 $\{a_1, \cdots, a_{k-1}, a_{k+1}, \cdots, a_m\}$ 将是生成元系.

这是很显然的, 因为由条件 $\sum\limits_{i \neq k} s_i a_i \pm a_k = 0$, 有 $a_k = \sum\limits_{i \neq k} s_i' a_i, s_i' = \pm s_i$, 于是其余 $m-1$ 个元生成 A.

c) 如果生成元系 $\{a_1, \cdots, a_m\}$ 的极小关系的高为 $h > 1$, 那么可以建立新的生成元系 $\{a_1', \cdots, a_m'\}$, 其极小关系的高严格小于 h.

事实上, 我们可以将生成元重新编号, 使 $|s_1| = \min|s_i| = h$. 如果必要, 在关系两边同乘 -1, 使 $s_1 = h$. 由 a) 知, 不是所有 s_i 都能被 h 整除. 利用再次重新编号, 可以认为 $h \nmid s_2 : s_2 = qh + r, 0 < r < h$. 那么我们的关系现在就变为

$$h a_1' + r a_2' + s_3 a_3' + \cdots + s_m a_m' = 0,$$

其中 $a_1' = a_1 + q a_2, a_i' = a_i, i > 1$. 显然 $\{a_1', a_2', \cdots, a_m'\}$ 将是一个生成元系, 其关系的高满足 $r < h$ (因为它的极小关系的高只能 $\leqslant r$).

现在用下列方法来证明我们定理的断言 1). 设 n 为群 A 的生成元个数的最小者且 $\{a_1, \cdots, a_n\}$ 是这样的一个生成元系. 我们也可以假设它的极小关系的高为 h (按所有势为 n 的生成元系).

如果 $h=1$, 那么由 b), 生成元的个数至少减少到 $n-1$, 这与我们的选择矛盾. 如果 $h>1$, 那么由 c), $\{a_1,\cdots,a_n\}$ 可以将一个极小关系变到更小 (也是势为 n 的生成元系) 的高. 该矛盾表明了, $\{a_1,\cdots,a_n\}$ 是无关的系, 从而是 A 的基.

2) 假设 $\{a_1,\cdots,a_m\},\{b_1,\cdots,b_n\}$ 为 A 的两组基. 两次引用引理 1, 就得到 $m\leqslant n$ 且 $n\leqslant m$. 于是 $n=m$. □

定义 有限生成交换群 A 称为**秩为 n 的自由群**且记为 F_n^{ab}, 如果

$$A=F_n^{ab}\cong\mathbb{Z}^n=\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}.$$

由一个零组成的群 A 的秩认为是零. 自由交换群 A 的任一基也称为它的一个**自由生成系**.

刚刚证明的定理说明, 任一有限生成无挠交换群 A 是一个秩为某个 n 的自由群.

事实上, 如果 $\{a_1,\cdots,a_n\}$ 是群 A 的一个基, 那么任意元 $a\in A$ 可以唯一地写成下列形式: $a=\alpha_1a_1+\cdots+\alpha_na_n,\alpha_i\in\mathbb{Z}$ (如果还有其它表示 $a=\alpha_1'a_1+\cdots+\alpha_n'a_n$, 那么我们有 $0=a-a_1=(\alpha_1-\alpha_1')a_1+\cdots+(\alpha_n-\alpha_n')a_n$. 由此得到 $\alpha_1'=\alpha_1,\cdots,\alpha_n'=\alpha_n$). 对应

$$a\mapsto(\alpha_1,\cdots,\alpha_n)$$

显然是群 A 与整数向量群 $\mathbb{Z}^n$ 的一个同构映射. 于是 A 是一个秩为 n 的自由群.

3. 有限秩的自由交换群 下列技术性特征的断言大大简化了自由交换群的子群和商群的研究.

定理 2 假设 B 为具有限秩 n 的自由交换群 A 的一个非零子群. 那么在 A 和 B 中可以选择相应的基 $\{a_1,\cdots,a_n\}$ 和 $\{b_1,\cdots,b_k\}$ 满足 $b_i=m_ia_i$, 其中 $m_i\geqslant 0$ 为非负整数, 且 $m_{i-1}|m_i,i=2,3,\cdots,k,k\leqslant n$ (可能 $m_{k+1}=\cdots=m_n=0$).

证明 在 A 中选取一个基 $\{v_1,\cdots,v_n\}$ 具有下列极值性质: B 含有元

$$b_1=m_1v_1+s_2v_2+\cdots+s_nv_n$$

带有最小的正系数 m_1. 这指的是, 对于其它有序元 v_i, 和 A 中任一其它基的选择或对于 B 中其它元 b, 其第一个正系数都不可能小于 m_1.

我们来验证此时的 $m_1|s_i,i=2,\cdots,n$. 事实上, 如果 $s_i=q_im_1+r_i,0\leqslant r_i<m_1$, 那么

$$b_1=m_1a_1+r_2v_2+\cdots+r_nv_n,$$

这里 $a_1=v_1+q_2v_2+\cdots+q_nv_n$. 易见 $\{a_1,v_2,\cdots,v_n\}$ 也是群 A 的一个基. 由 $\{v_1,\cdots,v_n\}$ 的极值性推得 $r_2=\cdots=r_n=0$, 于是 $b_1=m_1a_1$.

因为

$$b' = m_1a_1 + s_2v_2 + \cdots + s'_nv_n \in B \Longrightarrow m_1|m'_1,$$

且如果 $m'_1 = qm_1$, 那么

$$b'' = b' - qb_1 \in \langle v_2, \cdots, v_n\rangle,$$

即

$$A = \langle a_1\rangle \oplus A_1, \quad B = \langle b_1\rangle + B_1,$$

其中 $b_1 = m_1a_1, B_1 \subseteq A_1 := \langle v_2, \cdots, v_n\rangle$.

于是 B_1 是秩为 $(n-1)$ 的自由交换群 A_1 的子群, 直接对秩进行归纳, 我们得到对于 (A_1, B_1) 定理的断言成立, 即在 A 中存在元素 $a_2, \cdots, a_n$, 使得

$$A_1 = \langle a_2, \cdots, a_n\rangle, \quad B_1 = \langle b_2, \cdots, b_k\rangle, \quad b_i = m_ia_i, m_{i-1}|m_i, \quad i > 2.$$

而这只能是 $m_{k+1} = m_{k+2} = \cdots = m_n = 0$.

剩下的只需证明: $m_1|m_2$. 令 $m_2 = qm_1 + r, 0 \leqslant r < m$, 用 $a'_1 = a_1 + qa_2$ 替代 a_1. 相应于群 A 的基 $\{a'_1, a_2, \cdots, a_n\}$, 元素 $b_1 + b_2 \in B$ 有形式

$$b_1 + b_2 = m_1a_1 + (qm_1 + r)a_2 = m_1a'_1 + ra_2.$$

由此可见, 当 $r > 0$ 时, 得到一个与所选基的极值性或与 m_1 的选择的矛盾. 于是 $r = 0$. 定理证毕. □

在定理 2 的情况下, 人们说及 A 和 B 的基的相容性.

推论 1 秩为 n 的自由交换群 A 的任一子群是自由群, 其秩 $k \leqslant n$.

证明 由定理 2, 在群 $A, B \neq 0$ 中可以选取相应的基

$$A = \langle a_1, \cdots, a_n\rangle, \quad B = \langle b_1, \cdots, b_k\rangle, \quad b_i = m_ia_i, \quad 1 \leqslant i \leqslant k \leqslant n,$$

其中 $m_1|m_2, m_2|m_3, \cdots, m_{k-1}|m_k$ $(m_{k+1} = \cdots = m_n = 0)$. 于是任意元 $b \in B$ 可以写为

$$b = s_1m_1a_1 + s_2m_2a_2 + \cdots + s_km_ka_k.$$

如果存在不全为零的 $s_1, s_2, \cdots, s_k \in \mathbb{Z}$ 使得 $b = 0$, 那么我们将得到一个非平凡的线性相关的系 $\{a_1, \cdots, a_k\}$, 其系数为 $s_1m_1, s_2m_2, \cdots, s_km_k$, 这是一个矛盾, 因为 $\{a_1, \cdots, a_k\}$ 是群 A 的基的一部分. 于是群 B 的生成元系 $\{b_1, \cdots, b_k\}$ 无关 (或称自由), 从而 B 是秩 $k \leqslant n$ 的自由群. □

当 $n = 1$ 时推论 1 的断言, 当然是我们知道的: 群 $(\mathbb{Z}, +)$ 中的每个非零子群有形式 $m\mathbb{Z}$, 它也是一个无限循环群, 即秩为 1 的自由群.

推论 2 秩为 n 的自由交换群 A 的任一同态像 $\varphi(A)$ 同构于群

$$\mathbb{Z}^{n-k} \oplus Z_{m_1} \oplus \cdots \oplus Z_{m_k}, \quad 0 \leqslant k \leqslant n, \text{ 且 } m_{i-1}|m_i, \quad 2 \leqslant i \leqslant k.$$

证明 令 $B = \mathrm{Ker}\,\varphi$ 是同态 φ 的核. 由同态定理 (第 1 章 §4 定理 2), $\varphi(A) \cong A/B$. 我们来描写这个商群. 为此, 利用定理 2, 在 A 和 B 中选择相应的基. 设

$$A = A_1 \oplus \cdots \oplus A_n; \quad B = B_1 \oplus \cdots \oplus B_n,$$

其中

$$A_i = \mathbb{Z}a_i, \quad B_i = B \bigcap A_i = \begin{cases} n_i\mathbb{Z}a_i, & \text{当 } i \leqslant k, \\ 0, & \text{当 } i > k. \end{cases}$$

无限循环群 $\langle a_i \rangle = \mathbb{Z}a_i$ 关于子群 $m_i a_i \mathbb{Z}$ 的商群或者仍是群 $\langle a_i \rangle$ (当 $i > k$ 时), 或者是阶为 m_i 的循环群 $\langle \bar{a}_i | m_i\bar{a}_i = 0 \rangle$, 其同构于 $Z_{m_i}, i \leqslant k$.

由第 1 章 §4 定理 7, 我们有

$$A/B \cong A_1/B_1 \oplus \cdots \oplus A_k/B_k \oplus A_{k+1}/B_{k+1} \oplus \cdots \oplus A_n/B_n \cong Z_{m_1} \oplus \cdots \oplus Z_{m_k} \oplus \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n-k}.$$

□

4. 有限生成交换群的结构 定理 2 后面的推论实际上回答了有限生成交换群的基本问题. 我们现在首先来证明自由交换群的一个通用的性质.

引理 2 假设 X 是一个交换群 F 的生成元的集合, $|X| = n$. 那么下列断言等价:

i) $F = F_n^{ab}$ 是一个自由交换群且 X 是它的自由生成元集;

ii) 集合 X 到一个交换群 A 的每个单值映射 φ 诱导一个同态 $\tilde{\varphi}: F \to A$.

证明 i)$\Longrightarrow$ii). 设 $X = \{x_1, \cdots, x_n\}, \varphi: X \to A$. 因为 F 中的每个元可以唯一地写为 $\sum\limits_i s_i x_i$ 的形式, 所以显然, 映射

$$\tilde{\varphi}: \sum_i s_i x_i \mapsto \sum_i s_i \varphi(x_i)$$

是 F 到 A 的一个同态.

ii)$\Longrightarrow$i). 在这个蕴涵关系中, 我们立即知道 A 也是自由群, 它具有势与 X 的势相等的生成元集 $\{a_1, \cdots, a_n\}$. 如果 $\varphi: x_i \mapsto a_i$ 为按条件所说的单值映射, 并且它扩展为一个同态 $\tilde{\varphi}: F \to A$, 那么

$$\sum_i s_i x_i = 0 \Longrightarrow \sum_i s_i a_i = 0 \Longrightarrow s_i = 0,$$

即 $x_1, \cdots, x_n$ 是自由生成元且 $F = F_n^{ab}$. □

显然, 在引理 2 中集合 X 的有限性条件没有起任何作用, 而且我们也没有必要来讨论无限集.

定理 3　每个具有 n 个生成元的交换群是自由交换群 F_n^{ab} 的同态像.

证明　这是引理 2 的一个直接推论. □

结合定理 2 的推论 2 和定理 3, 我们得到这一节的一个基本结果.

定理 4　1) 任一有限生成交换群 A 是一个自由交换群 F_r^{ab} (其秩 $r \geqslant 0$) 与一个有限交换群的直和.

2) 任一有限交换群是 k 个阶为 $m_1, \cdots, m_k$ 的循环群的直和, 这里 k 为某个正整数, $m_{i-1}|m_i, 1 < i \leqslant k$.

5. 分类问题的其它方法　我们简略地介绍一下自由群的其它一些相关的结果.

引理 3　假设商群

$$A/B = \bigoplus_{i=1}^{n}(A_i/B)$$

是一个直和, 且 B 是每个子群 A_i 的直和项: $A_i = B \oplus J_i$. 那么 B 是 A 的直和项且

$$A = B \oplus \left(\bigoplus_{i=1}^{n} J_i\right).$$

证明　显然, B 和所有子群 J_i 生成 A, 假设 $b + x_1 + \cdots + x_n = 0$, 其中 $b \in B, x_i \in J_i$. 将它放入模 B 的商群, 得到

$$\overline{x}_1 + \cdots + \overline{x}_n = 0 \quad (\overline{x} = x + B).$$

但是因为 A_i/B 是 A/B 中的直和项, 所以 $\overline{x}_i = \bar{0}$, 于是, $x_i \in B$, 即 $x_i \in (B \cap J_i) = 0$, 而由这推出 $b = 0$, 这完成了我们的证明. □

定理 5　假设 A 是一个交换群, B 为 A 的一个子群. 如果商群 A/B 是自由群, 那么 A 是 B 和自由群 F^{ab} 的直和: $A = B \oplus F^{ab}$.

证明　因为 A/B 是无限循环群的直和, 所以由引理 4, 我们只需考虑这样的情况: $A/B \cong \mathbb{Z}$. 即

$$A/B = \langle \overline{a} \rangle \cong \mathbb{Z}.$$

取 $0 \neq a \in \overline{a}$ (不包含在 B 中的陪集 $\overline{a}$ 中的一个元). 那么元 ka 将是陪集 $k\overline{a}$ 的一个代表元, $k = 0, \pm 1, \pm 2, \cdots$, 即 $A = B \oplus \langle a \rangle$. □

定义　交换群 A 中所有有限阶元组成的子群 $T(A)$ 称为 A 的周期部分 (或称挠子群 —— 来自于英文 torsion subgroup).

很容易直接验证 $T(A)$ 是子群: 如果 $sa=0, tb=0; a,b\in T(A)$, 那么 $ts(\nu a+\mu b)=\nu t(sa)+\mu s(tb)=0$. 即 $\nu a+\mu b\in T(A)$.

引理 4 商群 $A/T(A)$ 是无挠群.

证明 假设 $\bar{a}=a+T(A)$ 是 $A/T(A)$ 中的有限阶元, 即 $m\bar{a}=ma+T(A)=\bar{0}$, 或者说 $ma\in T(A)$. 那么存在 $n\in\mathbb{Z}$ 使得 $n(ma)=0$. 但是, 如果 $(nm)a=0$, 那么由周期部分的定义知 $a\in T(A)$, 从而 $\bar{a}=\bar{0}$. □

现在假设 A 是一个具有 n 个生成元的交换群. 已如引理中所见到的, $A/T(A)$ 是一个无挠群. 它的生成元的个数显然不超过 n. 由定理 1, $A/T(A)\cong F_r^{ab}, r\leqslant n$, 是一个自由群. 再由定理 5 有分解

$$A=T(A)\oplus F_r^{ab}.$$

于是 $T(A)\cong A/F_r^{ab}$. 这表明, $T(A)$ 的生成元的个数同样不超过 n. 如果 $a_1,\cdots,a_s$ 为它的生成元且 $m_1a_1=\cdots=m_sa_s=0$ 那么显然 $T(A)$ 是阶 $\leqslant m_1\cdots m_s$ 的有限群. 于是我们得到下列断言.

定理 6 任意有限生成交换群 A 是有限交换群 $T(A)$ 与某个秩 r 的自由交换群 F_r^{ab} 的直和.

实际上我们也知道 (定理 4), $T(A)$ 是循环群的直和. 但我们想寻找其它的途径.

定理 7 任意周期交换群 A 可以分解为对应于不同素数 p 的 p–群 $A(p)$ 的直和. 直和项 $A(p)$ 由 A 唯一确定.

证明 设 $A(p)$ 由所有阶为素数 p 的方幂的元 $a\in A$ 组成 (可能 $A(p)=0$). 那么 $A(p)$ 是 A 的一个子群, 这因为 $p^kx=0=p^ly; x,y\in A, m=\max(k,l)\Longrightarrow p^m(x-y)=0\Longrightarrow x-y\in A(p)$.

每个 $A(p_1)+\cdots+A(p_s)$ 中的元的阶不可能被不同于 $p_1,\cdots,p_s$ 的素数 q 整除. 于是

$$A(q)\cap(A(p_1)+\cdots+A(p_s))=0.$$

这表明, 这些子群 $A(p)$ 生成一个直和 $\bigoplus\limits_p A(p)$ (按所有素数 p 求和).

剩下的只要证明, 群 A 由自己的 p–分量 $A(p)$ 生成. 假设 $a\in A$ 且 $|\langle a\rangle|=n=p_1^{k_1}\cdots p_r^{k_r}$, 这里 p_i 为不同的素数. 设 $n=n_ip_i^{k_i}, i=1,\cdots,r$. 那么这些整数 n_i 互素, 从而存在某些 $t_i\in\mathbb{Z}$ 使得

$$t_1n_1+\cdots+t_rn_r=1.$$

因此,

$$a=\sum_{i=1}^r t_i(n_ia),$$

其中 $n_ia \in A(p_i)$ (实际上, $p_i^{k_i}(n_ia) = na = 0$). 于是, 我们得到 $a \in A(p_1)+\cdots+A(p_r)$.

我们注意到, 在任一直和分解 $A = \bigoplus_p A'(p)$ 中, 不属于 $A'(p)$ 的任一个元不可能有阶 p^t, 于是 $A'(p) \supset A(p)$. 反之亦然, 于是 $A(p)$ 是唯一的. □

定理 8 (弗罗贝尼乌斯 –施蒂克贝格 (Frobenius-Stickelberger)) 每个有限交换群是有限多个素数幂阶循环群的直和.

证明 由定理 7, 可以只对有限 p–群加以证明, 而这一点本身具有独立意义.

设 A 为一个有限 p–群, $a \in A$ 是 A 的一个极大阶 p^k 的元. 那么循环群 $\langle a\rangle$ 是 A 的一个直和因子.

事实上, 令 B 为 A 的一个极大子群且有性质 $B \cap \langle a\rangle = 0$, 那么, 显然

$$H := \langle B, a\rangle = B \oplus \langle a\rangle.$$

假设 H 是 A 的一个真子群, 那么我们可以找到 $x \in A$ 满足 $x \notin H$, 但 $px \in H$ (如果 $p^ix \in H, p^{i-1}x \notin H$, 那么可用 $p^{i-1}x$ 代替 x). 于是

$$px = b + la \quad (b \in B, l \in \mathbb{Z}),$$

而且由 p^k 的极大性

$$p^{k-1}b + p^{k-1}la = p^kx = 0.$$

由此得到 $p^{k-1}la = 0$, 而这种情况下, $p^k|p^{k-1}l$, 即 $l = pj$, 对某个 $j \in \mathbb{Z}$. 现在对于 $y = x - ja$ 有 $py = b \in B$; 但是 $y \notin H$, 所以 $\langle B, y\rangle$ 包含 (由 B 的极大性) 非零元 $ra \in \langle a\rangle$.

那么, $ra = b' + sy; b' \in B, s \in \mathbb{Z}$. 由此得 $sy \in B + \langle a\rangle = H$. 如果 $p|s$, 那么 $sy \in B, b' + sy = b'' \in B$ 且 $0 \neq ra = b'' \Longrightarrow B \cap \langle a\rangle \neq 0$, 矛盾. 于是 $(s,p) = 1$, 且 $sy \in H, py \in H$, 由此得到 $y \in H$, 又得矛盾. 因此 $A = H, A = \langle a\rangle \oplus B$. 断言得证.

现在定理 8 的证明就显然了. 实际上, 在 A 中取极大阶 p^k 的元, 那么由上面证明的断言知 $A = \langle a\rangle \oplus B$. 对 B 继续这个过程, 因为 $|B| < |A|$, 最后得到定理的结论. □

下列定理为定理 8 的重要补充.

定理 9 如果一个有限交换 p–群 A 分解为两个不同的循环子群的直和:

$$A_1 \oplus \cdots \oplus A_r = A = B_1 \oplus \cdots \oplus B_s,$$

那么 $r = s$ 且适当调整次序可得阶 $|A_i|$ 等于 $|B_i|$.

证明 如果 $|A|=p$, 那么定理显然成立. 现在对 A 的阶 $|A|$ 运用归纳法. 为了方便, 我们一开始就调整次序使 A_i 和 B_j 的阶不增:

$$\begin{aligned}&A_i=\langle a_i\rangle,\quad |\langle a_i\rangle|=p^{\mu_i},\\&\mu_1\geqslant\mu_2\geqslant\cdots\geqslant\mu_q>\mu_{q+1}=\cdots=\mu_r=1;\end{aligned}\tag{3}$$

$$\begin{aligned}&B_j=\langle b_j\rangle,\quad |\langle b_j\rangle|=p^{\nu_j},\\&\nu_1\geqslant\nu_2\geqslant\cdots\geqslant\nu_t>\nu_{t+1}=\cdots=\nu_s=1.\end{aligned}\tag{4}$$

集合 $pA=\{px|x\in A\}$ 是 A 的一个子群, 且它不依赖于任何分解. 另一方面, 如果

$$i_1a_1+\cdots+i_qa_q+\cdots+i_ra_r=x=j_1b_1+\cdots+j_tb_t+\cdots+j_sb_s,$$

那么由 (3) 和 (4) 有

$$i_1(pa_1)+\cdots+i_q(pa_q)=x=j_1(pb_1)+\cdots+j_t(pb_t).$$

于是

$$\langle\widetilde{a}_1\rangle+\cdots+\langle\widetilde{a}_q\rangle=pA=\langle\widetilde{b}_1\rangle+\cdots+\langle\widetilde{b}_t\rangle,$$

其中 $\widetilde{a}_i=pa_i,\widetilde{b}_j=pb_j$ 的阶分别为 p^{μ_i-1} 和 p^{ν_j-1}. 因为 $|pA|<|A|$, 所以由归纳假设 $q=t$ 且 $\mu_1-1=\nu_1-1,\cdots,\mu_q-1=\nu_q-1$, 由此得到 $\mu_1=\nu_1,\cdots,\mu_q=\nu_q$. 同时注意到

$$|A_{q+1}+\cdots+A_r|=p^{r-q},\quad |B_{t+1}+\cdots+B_s|=p^{s-t},q=t,$$

我们得

$$p^{\mu_1+\cdots+\mu_q}p^{r-q}=|A|=p^{\mu_1+\cdots+\mu_q}p^{s-q},$$

于是 $s=r$. 定理证毕. □

6. 有限交换群的基本定理 为了表达多样性, 我们将给出有关有限交换群的乘法描述, 即用积代替和, 用因子代替加项, 而转为乘法的记号. 根据定理 7~9, 我们直接得到下列基本结果.

定理 10 任意有限交换群 A 是准素循环子群的直积. 在任意两个这样的分解中, 相同阶因子的个数相同.

借用向量空间的术语, 我们说阶为 $d_1,\cdots,d_r$ 的元 $a_1,\cdots,a_r$ 组成交换群 A 的基是指, 如果每个元 $x\in A$ 可以唯一地表示为下列形式

$$x=a_1^{i_1}a_2^{i_2}\cdots a_r^{i_r},\quad 0\leqslant i_k<d_k,k=1,\cdots,r.$$

当然, 在这种情况下

$$A=\langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_r\rangle,\quad |A|=d_1d_2\cdots d_r,\tag{5}$$

且定理 10 等价于这样的断言: 在任意有限交换群 A 中存在基, 且基的元是准素阶的 (也就是说, 阶 d_i 是一个素数 p 的幂, 这里 $p||A|$), 而且数组 $\{d_1,\cdots,d_r\}$ 与基的选取无关. 正由于如此, 数 $d_1,\cdots,d_r$ 称为群 A 的不变量或 A 的初等因子. 有时还称 $\{d_1,\cdots,d_r\}$ 为有限交换群 A 的型.

写出所有不变量, 按阶 $|A|$ 的不同素因子排成行:

$$\begin{array}{ll} p_1^{m_{11}},p_1^{m_{12}},\cdots, & p_1^{m_{1k}};\ m_{11}\leqslant m_{12}\leqslant\cdots\leqslant m_{1k};\\ p_2^{m_{21}},p_2^{m_{22}},\cdots, & p_2^{m_{2k}};\ m_{21}\leqslant m_{22}\leqslant\cdots\leqslant m_{2k};\\ \quad\cdots & \qquad\qquad\cdots\\ p_s^{m_{s1}},p_s^{m_{s2}},\cdots, & p_s^{m_{sk}};\ m_{s1}\leqslant m_{s2}\leqslant\cdots\leqslant m_{sk};\end{array}$$

如果在一些行中补充一些单位, 那么可以认为, 所有不变量的行有同样的长 k.

整数

$$m_i=p_1^{m_{1i}}p_2^{m_{2i}}\cdots p_s^{m_{si}},\quad i=1,2,\cdots,k,$$

称为交换群 A 的不变因式. 按照排列,

$$A=m_1m_2\cdots m_k,\quad m_{i-1}|m_i;\quad 1<i\leqslant k. \tag{6}$$

为了确信不变因式我们已经遇到过, 只需返回看看定理 2 的推论 2. 由展开式 (5), 并重新写为形式

$$A=(\langle a_{11}\rangle\times\cdots\times\langle a_{s1}\rangle)\times\cdots\times(\langle a_{1k}\rangle\times\cdots\times\langle a_{sk}\rangle),$$

我们又将得到分解式

$$A=\langle u_1\rangle\times\langle u_2\rangle\times\cdots\times\langle u_k\rangle. \tag{7}$$

其直因子是阶分别为 $m_1,m_2,\cdots,m_k$ 的循环群. 为此只需令

$$u_i=a_{1i}a_{2i}\cdots a_{si},\quad 1<i\leqslant k,$$

且应用命题 2 或断言 (1).

对于准素阶群 A, 直分解式 (5) 和 (7) 显然是相同的, 但在一般情况下, 分解式 (7) 比分解式 (5) 更加精练 ($k\leqslant r\leqslant sk$), 而且在 (7) 中分出元素 u_k 具有最高阶 $m:=m_k$; 群 A 中所有其它元的阶整除 m. 这个整数 m 也称为群 A 的幂指数. 一个交换群 A 是循环群当且仅当它的幂指数等于 A 的阶 $|A|$.

上面这最后的结论在证明下面有关域的有益结论中起着重要作用.

定理 11　设 F 是任意一个域, A 是乘法群 F^* 的一个有限子群, 那么 A 是循环群.

证明 假如 A 不是一个循环群, 那么由上面所说的有 $m < |A|$, 这里 m 是 A 的幂指数: $a^m = 1, \forall a \in A$. 在这种情况下多项式 $X^m - 1$ 在域 F 中就会有超过 m 个根, 而这是不可能的, 于是 A 是循环群. □

剩下补充的是, 还没有提到的关于具有给定不变因式 $m_1, m_2, \cdots, m_k$ 的交换群的存在性问题: 与前面一样, 只需考虑 (在加法交换群中) 循环群 $Z_{m_1}, \cdots, Z_{m_k}$ 的直和. 给定阶为 N 的互不同构的交换群的个数也许能写为相当明显的形式. 例如,阶为 $N = p^n$ (p 为一个素数) 的不同构的交换群的个数等于有序分解

$$n = n_1 + n_2 + \cdots + n_l, \quad n_1 \geqslant n_2 \geqslant \cdots \geqslant n_l, \quad 1 \leqslant l \leqslant n,$$

的个数 $p(n)$.

整数函数 $p(n)$ 已经在描写对称群 S_n 的共轭元素类时遇到过 (见第 1 章 §3 习题 4). 阶为 p^n 且指数为 p (即不变量为 $p, \cdots, p$) 的交换群称为**初等交换群**. 对于运算写成加法的交换群, 我们指出 $pA = 0$ (p 为一个素数) 的加法交换群是 p 个元的有限域 $\mathbb{F}_p$ 上的一个向量空间. 事实上, 如果我们把 $\mathbb{F}_p$ 中的元与模 p 的剩余类 $\bar{k}$ 认为相同 ($\mathbb{F}_p = Z_p$) 并让 $\bar{k}a := ka, a \in A$, 那么我们就得到一个 $\mathbb{F}_p$ 在 A 上的作用, 从而 A 就成为域 $\mathbb{F}_p$ 上的一个向量空间. 这个作用定义是合理的, 因为 $\bar{k} = \overline{k'}$ 推得 $(k - k')a = l(pa) = 0$. A 分解为循环子群的直和在向量空间中对应到一维子空间的直和 ([BA II] 第 1 章, 关于基的定理). 于是

$$A \cong Z_p^n = Z_p \oplus \cdots \oplus Z_p.$$

对于 $n = 2$ 时, 子空间的一维基的选择有多少种呢, 由第 1 章例子看到: Z_p^2 有 $p(p+1)$ 种.

例 4 作为例子列举阶为 16 和 36 的所有交换群:

$|A| = 16 = 2^4, p(4) = 5,$

$Z_{16}, \quad Z_8 \oplus Z_2, \quad Z_4 \oplus Z_4, \quad Z_4 \oplus Z_2 \oplus Z_2, \quad Z_2^4 = Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_2,$

$\|A\| = 36 = 2^2 \cdot 3^2$	初等因子	不变因式
$Z_4 \oplus Z_9 \cong Z_{36}$	4,9	36
$Z_2 \oplus Z_2 \oplus Z_9 \cong Z_2 \oplus Z_{18}$	2,2,9	18,2
$Z_4 \oplus Z_3 \oplus Z_3 \cong Z_3 \oplus Z_{12}$	4,3,3	12,3
$Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_3 \cong Z_6 \oplus Z_6$	2,2,3,3	6,6

例 5 我们来将群 $Z_{72} \oplus Z_{84}$ 写成不变因式对应的分解. 首先将它的每个循环加项表示为准素循环分量:

$$Z_{72} = Z_8 \oplus Z_9, Z_{84} = Z_4 \oplus Z_3 \oplus Z_7.$$

进一步将整个群写成按每个素数 p 合在一起的准素分量的分解:

$$Z_{72} \oplus Z_{84} = (Z_4 \oplus Z_8) \oplus (Z_3 \oplus Z_9) \oplus Z_7$$

(即西罗 p–子群的直和). 现在再在每个准素分量中各选出一个最小阶的直和项, 并对余下的加项重复这个过程得到

$$Z_{72} \oplus Z_{84} = (Z_4 \oplus Z_3) \oplus (Z_8 \oplus Z_9 \oplus Z_7) = Z_{12} \oplus Z_{504}.$$

如果对群 $Z_{36} \oplus Z_{168}$ 进行上面同样的进程, 那么会得到类似的结果. 于是

$$Z_{72} \oplus Z_{84} = Z_{36} \oplus Z_{168}$$

(严格地讲, 应该用 $\cong$ 代替等号). 特别地, 我们指出两个群的指数等于 504.

习 题

1. 证明: 在有限交换群 A 中, 对于任意 $d \mid |A|$, 至少存在一个阶为 d 的子群 (拉格朗日定理的逆).
2. 证明: 在适当的次序下, 交换群的任一子群的不变量是群的不变量的因子.
3. 如果 $A \oplus A \cong B \oplus B$, 这里 A 和 B 为有限交换群, 那么 $A \cong B$.
4. 如果 A, B, C 是有限交换群且 $A \oplus C \cong B \oplus C$, 那么 $A \cong B$.
5. 如果一个正整数 n 不能被 > 1 的整数的平方整除, 那么任一阶为 n 的有限交换群一定是循环群.
6. 写出阶为 72 的所有不同构的交换群.
7. 群 $Z_{12} \oplus Z_{72}$ 与 $Z_{18} \oplus Z_{48}$ 同构吗?
8. 试用整数矩阵 (系数属于 $\mathbb{Z}$ 的矩阵) 的语言准确地表达并证明有限生成交换群的定理. 在这样的矩阵上用适当的方法进行初等变换.
9. 证明: 秩为 n 的自由交换群 F_n^{ab} 的子群 A 的指数是有限的充分必要条件是 $\operatorname{rank} A = n$.

§4 线性李群

1. 定义和例子 形式地说, 一个赋予群结构, 同时具有一个光滑映射, 即乘法 $(x, y) \mapsto xy$ 及取逆元 $x \mapsto x^{-1}$ 的微分流形 (C^2 或甚至 C^∞ 类, 光滑的), 称为**李群**.

李群 G 到李群 H 的同态 $\Phi : G \to H$ 同时要求一个流形到另一个流形的映射的光滑性. 对于李群的同构、自同构的概念有同样要求. 常常遇到的是实流形和复流形以及相应的实李群和复李群.

因为流形的构造表达是以拓扑为前提的, 所以李群是拓扑群. 这表明, 积 gh 和取逆 g^{-1} 在给定的拓扑中是连续运算. 拓扑空间的连通性、局部连通性和紧性的概

念将认为是熟悉的. 特别地, 一个群称为紧的, 如果对于相应的拓扑空间, 博雷尔 –勒贝格 (Borel-Lebesgue) 定理成立.

严格的李群定义, 合并了通常群的概念、拓扑空间的概念和微分流形的概念, 比较复杂. 并且**李群**的定义假设了 H 是一个**子流形** (新概念), 规定在单位元 $(e \in H)$ 的邻域用 G 上的局部坐标 $x_1, \cdots, x_n$, 它们满足方程组

$$f_i(x_1, \cdots, x_n) = 0, \quad 1 \leqslant i \leqslant m. \tag{1}$$

认为

$$\operatorname{rank}\left(\frac{\partial f_i}{\partial x_j}\right)_e = m.$$

在方程组 (1) 上这个条件, 用平移变到任意点 $h \in H$, 给 H 提供了 $(n-m)$-维流形的结构. 同时指出, 李群 G 常常在单位元 $e \in G$ 的适当邻域被局部地研究. 详细研究这些是出格的, 因为我们的兴趣是典型线性群, 所以这一章从刚一开始可以认为它们是李群, 而对许多一般定义置之不理.

例 1 $(\mathbb{R}^n, +)$ 是李群.

例 2 设 V 是 $\mathfrak{K}(\mathfrak{K} = \mathbb{R}$ 或 $\mathfrak{K} = \mathbb{C})$ 上的一个有限维向量空间. 我们知道向量空间 V 的自同构群 $\operatorname{Aut} V$ 是具有条件 $\det \neq 0$ 的 $\operatorname{Hom}(V, V)$ 中的一个开子集. 所以 $\operatorname{Aut} V$ 是一个光滑流形. 自同构的自然合成是一个光滑映射: 如果 $A = (a_{ij}), B = (b_{jk})$, 那么 $AB = C = (c_{ik})$, 其中 $c_{ik} = \sum_j a_{ij} b_{jk}$. 类似地, 映射 $x \mapsto x^{-1}$ 是光滑的: 只要回忆克拉默 (Cramer) 公式. 于是 $\operatorname{Aut} V$ 是一个维数为 n^2 的李群. 它在 $\mathfrak{K}$ 上的矩阵表示我们采用符号 $\mathrm{GL}(n, \mathfrak{K})$ 或 $\mathrm{GL}_n(\mathfrak{K})$.

例 3 对于群 $\mathrm{SL}(n, \mathfrak{K})$, 方程组 (1) 简化为等式

$$\det X = 1, X = (x_{ij}) \in \mathrm{GL}(n, \mathfrak{K}),$$

显然满足条件 $\partial(\det X)/\partial x_{11}|_{X=E} = 1$. 因此 $\mathrm{SL}(n, \mathfrak{K})$ 是一个 $(n^2 - 1)$ 维李群.

例 4 由 [BA II] 第 3 章知, 正交群 $\mathrm{O}(n) \subset \mathrm{GL}(n, \mathbb{R})$ 由数量为 $m = n(n+1)/2$ 个下列双线性关系给定

$$f_{ij}(x) = \sum_k x_{ik} x_{jk} = \delta_{ij}.$$

容易验证, 变量为 $x_{st}, s \leqslant t$ 的矩阵 $(\partial f_{ij}/\partial x_{st})$ 的 m 阶子式在点 E 不同于零. 这表明 $\mathrm{O}(n)$ 是维数为 $n^2 - m = n(n-1)/2$ 的李群.

在单位元邻域与 $\mathrm{O}(n)$ 一致的子群 $\mathrm{SO}(n)$ 也有同样的维数. 更准确地说, 作为拓扑空间 $\mathrm{O}(n)$ 被分解为两个连通分支: 一个包含 E, 另一个包含 $-E$. 显然, 对于任意矩阵 $X \in \mathrm{O}(n)$, 有 $\det X = 1$.

例 5　在 [BA II] 第 3 章中, 酉群 $\mathrm{U}(n) \subset \mathrm{GL}(n,\mathbb{C})$ 的定义会与群 $\mathrm{O}(n)$ 的定义类似, 如果在 $\mathrm{GL}(n,\mathbb{C})$ 上看成关于 $2n^2$ 个参数的实数群上的话. $n(n+1)/2$ 个半拓扑关系的实部和虚部的划分产生 $2n(n-1)/2+n=n^2$ 个光滑函数. 对应的矩阵在点 $X=E$ 的秩也等于 n^2. 因此 $\mathrm{U}(n)$ 是维数为 $2n^2-n^2=n^2$ 的李群.

因为 $\det X = e^{i\varphi}, X \in \mathrm{U}(n), \varphi \in \mathbb{R}$, 所以 $\mathrm{SU}(n)$ 是一个维数为 n^2-1 的李群.

2. 矩阵群中的曲线　在拓扑线性空间中谈论曲线、切向量等是有意义的. 在分析和几何中有限维实向量空间 V 中的曲线被理解为一个连续映射 (函数) $\Gamma : (\alpha,\beta) \to V$, 其中 (α,β) 为 $\mathbb{R}$ 中一个区间. 比如, 曲线 $\varphi \mapsto (\cos\varphi, \sin\varphi), \varphi \in [0,2\pi)$, 其实就是中心经过直角坐标系原点的单位圆. 当然, V 常常被赋予仿射空间或欧几里得空间的结构. 令 $V = \langle \mathbf{e}_1, \cdots, \mathbf{e}_n \rangle$. 以参数式 $\Gamma_t = (\gamma_1(t_1), \cdots, \gamma_n(t))$ 给定一个曲线, 这里, 对任意 $i=1,\cdots,n, \gamma_i(t)$ 是实值函数. 曲线 Γ 在点 $t \in (\alpha,\beta)$ 是可微的, 如果所有 $\gamma_i(t)$ 可微, 即存在导数 $\gamma_1'(t), \cdots, \gamma_n'(t)$ 且

$$\Gamma_t' := \frac{d\Gamma_t}{dt} = (\gamma_1'(t), \cdots, \gamma_n'(t))$$

是 V 中唯一确定的向量, 其称为 Γ 在 Γ_t 处的切向量或在时间 t 时的速度向量. 下面我们将讨论光滑曲线 Γ_t, 为简单起见, 将函数和它的值混为一谈.

现在令 $V = M_n(\mathbb{R})$ 或 $M_n(\mathbb{C})$, 并将它们分别看作为维数为 n^2 和 $2n^2$ 的向量空间. 我们将认为空间 $M_n(\mathfrak{K})(\mathfrak{K} = \mathbb{R}$ 或 $\mathbb{C})$ 上的曲线 Γ_t 实际上整个地在矩阵群 $G \subset M_n(\mathfrak{K})$ 中, 即 $\Gamma_t \in G, \forall t \in (\alpha,\beta)$. 于是, 自然地谈论群 G 中的曲线或群 G 上的曲线. 对于任意 $t=t_0$, 应当清楚地想象 A_{t_0} 是 n^2–维矩阵空间中曲线的一点. 如果 $A_t = (a_{ik}(t)), B_t = (b_{kj}(t)) : (\alpha,\beta) \to G$ 是群 G 中的两个参数曲线, 那么可以定义它们的乘积 $C_t = A_t B_t$:

$$C_t = (c_{ij}(t)), \quad c_{ij}(t) := \sum_{k=1}^{n} a_{ik}(t) b_{kj}(t), \quad t \in (\alpha,\beta). \tag{2}$$

我们首要的任务是去研究在典型矩阵群中所有经过单位元 E 的可微曲线的集合, 和在选出来点的曲线的所有切向量的集合. $M_n(\mathbb{C})$ 可解释为维数为 $2n^2$ 的实空间.

定理 1　假设 $G \subset \mathrm{GL}(n,\mathfrak{K})$ 为一个矩阵群, 那么下列断言成立.

i) 如果 $A_t, B_t : (\alpha,\beta) \to G$ 是 G 中的两个可微曲线, 那么它们的积 $C_t = A_t B_t$ 同样是可微的且

$$\frac{dC_t}{dt} = (A_t B_t)' = A_t' B_t + A_t B_t'.$$

ii) 令 $T = L(G)$ 是 G 中曲线 A_t (满足 $A_0 = E$) 的所有切向量 A_0' 的集合 (在参数 $t=0$ 的小邻域内). 那么 $L(G)$ 是 $M_n(R)$ 中的向量子空间.

证明 断言 i) 从定义关系 (2) 直接微分得到.

ii) 设 $A_0', B_0' \in T$. 那么 $(AB)_0 = A_0B_0 = EE = E$, 且由 i), 在 T 中包含向量 $(AB)_0' = A_0'B_0 + AB_0' = A_0'E + EB_0' = A_0' + B_0'$. 所以 T 是一个加群.

如果现在 λ 是一个纯量且 $A_0' \in T$, 那么我们来看在 $t=0$ 邻域的曲线 $B_t = A_{\lambda t}$. 显然 $B_0 = A_0 = E$, 而且 B_t 可微且 $B_0' = \lambda A_0'$. 因为由条件 $B_0' \in T$, 于是 $\lambda A_0' \in T$.□

定义 向量空间 $T = L(G)$ 称为群 G **在点** E **的切空间**.

例 6 设 $G = \mathrm{GL}(n, \mathbb{R})$. 因为 $\det : G \to \mathbb{R}$ 是一个连续函数且 $\det E = 1$, 所以可以指定一个小 $\varepsilon > 0$ 和一个中心在 E 点的半径为 ε 的球体, 使得在这个球体中的每个矩阵 A 满足不等式 $\det A \neq 0$, 即 $A \in G$. 现在对于任一矩阵 $B \in M_n(\mathbb{R})$ (即对于 n^2 维实向量空间中的任一向量), 我们用下列等式定义 $M_n(\mathbb{R})$ 中的一个曲线 B_t :

$$B_t = tB + E.$$

我们有 $B_0 = E, B_0' = B$, 而对小的 t, B_t 属于 G, 于是, 切空间 $L(\mathrm{GL}(n, \mathbb{R}))$ 等于 $M_n(\mathbb{R})$ 且具有维数 n^2. 类似可证, 切空间 $L(\mathrm{GL}(n, \mathbb{C}))$ 在 $\mathbb{R}$ 上有维数 $2n^2$.

例 7 对于群 $\mathrm{SL}(n, \mathbb{R})$, 我们应该在中心为 E 点的 ε–球体中选择具有 $\det A = 1$ 的矩阵 A, 而对于迹为零的任一矩阵 $B \in M_n(\mathbb{R})$ 和小参数 t, 利用矩阵指数 ([BA II] 第 7 章 §1) 来定义曲线 B_t :

$$B_t = \exp(tB).$$

于是 $B_0 = E, B_t' = B\exp(tB), B_0' = B, \det B_t = \exp(\mathrm{tr}(tB)) = 1$. 这表明, 切空间 $L(\mathrm{SL}(n, \mathbb{R}))$ 有维数 $n^2 - 1$.

例 8 由例 4 可见, 流形 (李群) 的切空间 $\mathrm{O}(n)$ 和 $\mathrm{SO}(n)$ 在点 E 是相等的. 现在令 B_t 是 $\mathrm{SO}(n)$ 中的任一曲线, 其在 E 点的切向量为 B_0'. 因为由定义 $B_s {}^tB_s = E$, 所以微分法导致关系 $B_0 + {}^tB_0 = 0$, 这表明, 任一切向量是斜对称的.

另一方面, 如果 A 是一个任一斜对称矩阵, 那么从 E 点 $(A_0 = E)$ 引出的曲线 $A_s = \exp(sA)$ 在 E 点的切向量 $A_0' = A$. 曲线 A_s 的每个点是一个行列式为 1 的正交矩阵 ([BA II] 第 7 章). 于是, $L(\mathrm{SO}(n) = \mathfrak{so}(n)$ 是一个维数为 $n(n-1)/2$ 的空间, 它由所有斜对称矩阵组成.

例 9 在酉群 $\mathrm{U}(n)$ 的情况下, 替代 $\mathfrak{so}(n)$ 的是 ($\mathbb{R}$ 上) 斜埃尔米特矩阵的空间 $\mathfrak{su}(n)$, 并利用在例 8 中的方法讨论, 我们能够确信 $L(\mathrm{U}(n))$ 有维数 n^2.

线性李群的维数早先的定义为给定的基本微分流形的无关参数的个数. 现在我们看到下列定理正确.

定理 2 假设 G 是典型线性李群 $\mathrm{GL}(n, \mathfrak{K}), \mathrm{SL}(n, \mathfrak{K}), \mathrm{O}(n), \mathrm{SO}(n), \mathrm{U}(n), \mathrm{SU}(n)$ (这里 $\mathfrak{K} = \mathbb{R}$ 或 $\mathfrak{K} = \mathbb{C}$) 之一, $L(G)$ 是它们在 E 点的切空间. 那么 $\dim G = \dim L(G)$.

证明 对照例 2–5, 6–9 即得. □

讲了定理中的一些群, 本当接着补充讲辛群, 但为了叙述简单起见, 我们约定省去它.

3. 同态的微分 在群 H 中的曲线 $(\Phi\circ\Gamma)_t=\Phi(\Gamma_t)$ 适合矩阵群 G 和 H 的任一同态 $G\to H$ 和群 G 中任一光滑曲线 A_t. 如果所有曲线 $\Phi\circ\Gamma_t$ 光滑, 那么同态 Φ 自然称为光滑的.

定义 规定

$$d\Phi\left(\Gamma_0'\right)=(\Phi\circ\Gamma)_0', \tag{3}$$

那么矩阵李群的光滑同态 $\Phi:G\to H$ 和 G 在点 E 的切向量 Γ_0' 可以认为与 H 在 E 的切向量 $d\Phi\left(\Gamma_0'\right)$ 一致.

等式 (3) 所给的映射 $d\Phi:L(G)\to L(H)$ 称为同态 Φ 的**微分**或**切映射**.

定理 3 在矩阵群中下列断言成立:

i) 群同态的微分是切空间的线性映射.

ii) 如果 $\Phi:G\to H,\Psi:H\to K$ 为光滑同态, 那么

$$d(\Psi\Phi)=d\Psi\cdot d\Phi.$$

iii) 光滑同态 $\Phi:G\to H$ 给出线性同构 $d\Phi:L(G)\to L(H)$, 并且 $\dim G=\dim H$.

证明 假设 $A_0',B_0'\in L(G),\mu,\nu\in\mathbb{R}$, 那么

$$\begin{aligned}d\Phi(\mu A_0'+\nu B_0')&=(\Phi\circ(\mu A+\nu B))_0'=(\mu(\Phi\circ A)+\nu(\Phi\circ B))_0'\\&=\mu(\Phi\circ A)_0'+\nu(\Phi\circ B)_0'=\mu d\Phi(A_0')+\nu d\Phi(B_0').\end{aligned}$$

这表明断言 i) 成立.

为了证明 ii), 我们首先指出, 合成 $\Psi\Phi$ 是一个光滑同态, 于是表达式 $d(\Psi\Phi)$ 有意义且

$$d(\Psi\Phi)(A_0')=((\Psi\Phi)\circ A)_0'=d\Psi(\Phi\circ A)_0'=d\Psi\circ d\Phi(A_0').$$

最后, $d\Phi$ 的同构性由下列考虑得出. 因为 $\Phi^{-1}\Phi$ 是一个恒等映射, 所以由 ii) 有恒等映射 $d\Phi^{-1}\cdot d\Phi:L(G)\to L(G)$, 于是 $d\Phi$ 是一个单射, 而 $d\Phi^{-1}$ 是一个满射. 但是 $\Phi\Phi^{-1}$ 同样也是恒等映射, 于是 $d\Phi^{-1}$ 是单射, 而 $d\Phi$ 是满射. 这给出了所有需要的证明. □

我们不加证明地给出有关李群的下列内容丰富的定理, 详情请读者参看 [34].

定理 4 连通李群到任意李群的同态由自己的微分唯一确定.

4. 李群的李代数 由 [BA II] 我们已经知道什么是李代数$\mathfrak{L}$. 因为 $\mathfrak{L}$ 中元素 x,y 的积采用符号 $[\mathbf{x},\mathbf{y}]$, 那么对于李群 G 中元素 g,h 的换位子我们通常用符号 $(g,h)=ghg^{-1}h^{-1}$ 来表示. 回想一下, 李代数的括积 (或称换位子) 对每个变量是线性的, 括积也是斜对称的且满足雅可比 (Jacobi) 恒等式

$$[[\mathbf{x},\mathbf{y}],\mathbf{z}]+[[\mathbf{y},\mathbf{z}],\mathbf{x}]+[[\mathbf{z},\mathbf{x}],\mathbf{y}]=0. \tag{4}$$

由例 6～9 和 [BA II] 第 7 章, 我们知道, 典型线性李群的切空间具有李代数的结构. 不过, 可资借鉴地看看群的通常乘法与对应的李群的括积之联系, 以及在一般情况下, 与李群的联系.

假设 G 是一个具有单位元 e 的连通李群, $L(G)$ 是 G 在 e 点处的切空间. 由 $e:g_0=e=h_0$ 引出的曲线 $g_t,h_s,0\leqslant s,t\leqslant 1$, 的切向量 $g_0',h_0'\in L(G)$ 在 G 上的换位子 $[g_0',h_0']$ 用下列关系定义

$$[g_0',h_0']:=\left.\frac{\partial^2}{\partial t\partial s}(g_t,h_s)\right|_{t=s=0}. \tag{5}$$

置

$$f(t,s)=(g_t,h_s),$$

我们看到, $f(t,0)=e$ 且

$$q_t'=\left.\frac{\partial}{\partial s}f(t,s)\right|_{s=0}\quad\in L(G)$$

是曲线 $q:s\to f(t,s)$ 的切向量, 而

$$\left.\frac{\partial^2}{\partial t\partial s}f(t,s)\right|_{t=s=0}$$

是空间 $L(G)$ 中曲线 q_t' 的切向量. 群 G 具有坐标 $(x_1,\cdots,x_n)$ 与 $(y_1,\cdots,y_n)$ 的 n 维元的换位子 (Γ_t,Δ_s) 可以通过可微函数 $f_i(x_1,\cdots,x_n,y_1,\cdots,y_n)(1\leqslant i\leqslant n)$ 来表示. 函数 f_i 的形式完全由群确定而不依赖于具体的元素, 因此, 对于换位子 $[g_0',h_0']$ 我们有下列明显的表达式

$$[g_0',h_0']_t=\sum_{j,k}\left.\frac{\partial^2 f_i}{\partial x_j\partial y_k}\right|_{(e,e)}(g_0')_j\,(h_0')_k\,. \tag{6}$$

由 (6) 可见, 在 (5) 中的偏导数不依赖于坐标的选取, 而换位子关于每个变量是线性的.

如果采用容易验证的关系 $(a,b)=(b,a)^{-1}$, 那么可以证明, 换位子 (5) 是斜对称的. 恒等式 (4) 证明起来有点困难, 但是如果改为考虑线性李群 (不一定是典型群), 即令 $L(G)\subset M_n(\mathfrak{K}),\mathfrak{K}=\mathbb{R}$ 或 $\mathfrak{K}=\mathbb{C}$, 那么事情就简化了. 对于任意两个矩阵

$X,Y\in L(G)$ (它们是曲线 $\exp(tX),\exp(sY)\in G$ 的切向量), 直接计算幂级数, 并精确到次数为 3 的项, 有

$$\exp(tX)\exp(sY)=E+tX+sY+tsXY+\frac{t^2}{2}X^2+\frac{s^2}{2}Y^2+\cdots\in G,$$

于是

$$\begin{aligned}(\exp(tX),\exp(sY))&=\left(E+tX+sY+tsXY+\frac{t^2}{2}X^2+\frac{s^2}{2}Y^2+\cdots\right)\\&\quad\times\left(E-tX-sY+tsXY+\frac{t^2}{2}X^2+\frac{s^2}{2}Y^2+\cdots\right)\\&=E+ts(XY-YX)+t^2sU(X,Y,t,s)+ts^2V(X,Y,t,s),\end{aligned}$$

其中 $\deg_{X,Y}U(X,Y,t,s)\geqslant 3,\deg_{X,Y}V(X,Y,t,s)\geqslant 3$. 现在由公式 (5) 得到

$$[X,Y]=\frac{\partial^2}{\partial t\partial x}(E+ts(XY-YX)+t^2sU(X,Y,t,s)+ts^2V(X,Y,t,s))|_{t=s=0}=XY-YX,$$

也就是说, 由抽象方式定义的换位子 $[X,Y]$ 变为我们以前采用的自然表达式 $[X,Y]=XY-YX$.

雅可比恒等式对于这样括积表达式也满足. 于是我们得到

定理 5 任一线性李群的切代数由具有括积 $[X,Y]=XY-YX$ 运算的李代数的结构所提供.

5. 对数 对于足够接近 E 的任一实 $n\times n$ 矩阵 X 所确定的对数映射

$$\log X=(X-E)-\frac{(X-E)^2}{2}+\frac{(X-E)^3}{3}-\frac{(X-E)^4}{4}+\cdots,\tag{7}$$

给出了矩阵群中的指数映射 $\exp:L(G)\to G$. 为了证实这一点, 我们令 $Y:=X-E=(y_{ij})$, 并认为 $|y_{ij}|<\varepsilon$. 简单的对 k 归纳可知 $|(Y^k)_{ij}|\leqslant n^{k-1}\varepsilon^k$, 于是对于 (7) 式中两个相邻项的模关系, 我们有

$$\frac{|(Y^{k+1})_{ij}|}{|(Y^k)_{ij}|}\frac{k}{k+1}\frac{n^k\varepsilon^{k+1}}{n^{k-1}\varepsilon^k}=\frac{k}{k+1}n\varepsilon.$$

因此, 对于具有 $|(X-E)_{ij}|<1/n$ 的任意矩阵 X, 列 (7) 收敛.

定理 6 假设 U_E 是 E 在 $M_n(\mathbb{R})$ 中的一个邻域, 其中定义了映射 log, 而 U_0 为零的一个邻域满足 $\exp(U_0)\subset U_E$, 那么

i) $\exp\log X=X,\quad X\in U_E;\quad \log\exp Y=Y,\quad Y\in U_0$.

ii) 如果 A,B 可交换且邻近于 E, 那么

$$\log(AB)=\log A+\log B.$$

证明 i) 与数的情形没有什么区别. 对于 ii), $\exp(\log(AB)) = AB = (\exp(\log(A)) \cdot (\exp(\log B)) = \exp(\log A + \log B)$. 剩下的是运用 exp 在 0 附近的双射性.

个别说明 1) 称光滑同态 $\sigma : \mathbb{R} \to G$ 为线性李群 G 的**单参数子群**. 因为 $\sigma(t) = (\sigma(t/n))^n$, 所以 σ 由自己在 $0 \in \mathbb{R}$ 附近的值所确定. 在 [BA II] 第 7 章, 由 2 阶方阵 A 所确定的单参数群 $\sigma : t \mapsto \exp(tA)$ 的例子, 在某种意义讲是一般的, 因为曲线 $\exp(tA), A \in L(G)$, 局部地生成 G.

2) 在李群的线性表示下理解可微同态 $\Phi : G \to \mathrm{GL}(V)$, 其中 V 是 $\mathbb{R}$ 上或 $\mathbb{C}$ 上的向量空间. 矩阵 Φ_g 的系数按定义是 $g \in G$ 的一个可微函数, 在 G 和 V 中的具备实结构或复结构有一些不同的表现方式 (参见, 例如, [1]). 紧李群的线性表示实际上由对应的李代数的表示所确定. 在第 3 章中群 SU(2) 和它的李代数 $\mathfrak{su}(2)$ (第 4 章) 的描写是很好的例证.

习 题

1. 证明: 对于群 $\mathrm{GL}(n, \mathbb{R})$ 的每一个单参数子群 σ, 存在一个矩阵 $A \in M_n(\mathbb{R})$, 满足 $\sigma(t) = \exp(tA)$.

2. 给定线性李群 G 的李代数 $L(G)$ 的自同构, 其自身也形成一个线性李群 $\mathrm{Aut}(L(G))$. 如果 Γ_t 是 $\mathrm{Aut}(L(G))$ 中的某一个曲线, 那么 $\Gamma_t[\mathbf{a}, \mathbf{b}] = [\Gamma_t \mathbf{a}, \Gamma_t \mathbf{b}]$. 在 $t = 0$ 时的微分, 采用记号

$$\mathcal{D} = \left(\frac{d}{dt} \Gamma_t \right)_{t=0} \quad (认为\ \Gamma_0 = E),$$

得到

$$\mathcal{D}[\mathbf{a}, \mathbf{b}] = [\mathcal{D}\mathbf{a}, \mathbf{b}] + [\mathbf{a}, \mathcal{D}\mathbf{b}],$$

该关系允许我们称 $\mathcal{D}$ 为李代数 $L(G)$ 的微分. 这个概念我们已经在 [BA II] 中见过.

证明: 如果 $\mathcal{D}$ 是李代数 $L(G)$ 的微分, 那么 $\exp \mathcal{D}$ 是它的自同构.

第 3 章　表示论基础

在给出群的线性表示理论的准确定义之前, 我们首先讲两个问题.

问题 1　在 m 次实齐次多项式

$$f(x,y) = a_0x^m + a_1x^{m-1}y + \cdots + a_{m-1}xy^{m-1} + a_my^m$$

(或简洁地说, 多项式函数 $(x,y) \mapsto f(x,y)$) 组成的 $(m+1)$ 维空间 V_m 中, 由偏导数带来 2 维拉普拉斯方程

$$\frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2} = 0 \tag{$*$}$$

的解的集合 (见 [BA I], 第 6 章 §1 习题 9). 拉普拉斯算子 $\Delta = \dfrac{\partial^2}{\partial x^2} + \dfrac{\partial^2}{\partial y^2}$ 满足

$$\Delta(\alpha f + \beta g) = \alpha \Delta f + \beta \Delta g, \quad \forall \alpha, \beta \in \mathbb{R}.$$

因此方程 $(*)$ 的解构成空间 V_m 的一个子空间 H_m. 直接验证知

$$\Delta f = \sum_{k=0}^{m-2} [(m-k)(m-k-1)a_k + (k+2)(k+1)a_{k+2}]x^{m-k-2}y^k.$$

于是,

$$\Delta f = 0 \Longleftrightarrow (m-k)(m-k-1)a_k + (k+2)(k+1)a_{k+2} = 0, \quad 0 \leqslant k \leqslant m-2,$$

且所有系数 a_i 可以由它们中的 2 个表示, 譬如说, 由 a_0 和 a_1. 因此, $\dim H_m \leqslant 2$.

然而两个线性无关的解可以随之确定. 事实上, 按照算子 Δ 的线性作用扩充到复系数多项式, 我们有

$$\Delta(x+iy)^m = m(m-1)(x+iy)^{m-2} + imi(m-1)(x+iy)^{m-2} = 0, \quad i^2 = -1.$$

区分实部与虚部, 得到

$$z_m(x,y) = (x+iy)^m = u_m(x,y) + iv_m(x,y),$$

由

$$\Delta u_m + i\Delta v_m = \Delta z_m = 0 \Longrightarrow \Delta u_m = 0, \quad \Delta v_m = 0.$$

于是,

$$H_m = \langle u_m(x,y), v_m(x,y)\rangle_{\mathbb{R}}.$$

现在将 x, y 解释为具有固定直角坐标系的欧几里得平面 $\mathbb{R}^2$ 中向量的坐标, 我们来看在坐标的正交变换 (即平面 $\mathbb{R}^2$ 绕原点按任意角 θ 的旋转) 下所发生的:

$$x' = \Phi_\theta(x) = x\cos\theta - y\sin\theta,$$
$$y' = \Phi_\theta(y) = x\sin\theta + y\cos\theta.$$

由分析 (对于多项式易于验证) 中所熟悉的复合函数微分法, 我们有

$$\frac{\partial^2 f}{\partial x'^2} = \frac{\partial^2 f}{\partial x^2}\cos^2\theta - 2\frac{\partial^2 f}{\partial x\partial y}\cos\theta\cdot\sin\theta + \frac{\partial^2 f}{\partial y^2}\sin^2\theta,$$
$$\frac{\partial^2 f}{\partial y'^2} = \frac{\partial^2 f}{\partial x^2}\sin^2\theta + 2\frac{\partial^2 f}{\partial x\partial y}\cos\theta\cdot\sin\theta + \frac{\partial^2 f}{\partial y^2}\cos^2\theta,$$

由此得到

$$\frac{\partial^2 f}{\partial x'^2} + \frac{\partial^2 f}{\partial y'^2} = \frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2}.$$

这就是说, 方程 (*) 在变量的正交变换下, 或者说, 在群 $SO(2) = \{\Phi_\theta\}$ 的作用下, 是不变的. 其中, 多项式 $u_m(x', y'), v_m(x', y')$ 是方程 (*) 的解且它们本身可由 $u_m(x,y), v_m(x,y)$ 线性表示. 于是, 群 SO(2) 作用在拉普拉斯方程的解空间上. 在这种情况下, 人们谈论群 SO(2) 的 2 维实线性表示

$$\Phi^{(m)} : \Phi_\theta \mapsto \Phi^{(m)}(\theta).$$

再转回复多项式, 我们注意到

$$x' + iy' = xe^{i\theta} + iye^{i\theta} = e^{i\theta}(x+iy),$$
$$(x'+iy')^m = e^{im\theta}(x+iy)^m.$$

保留复化线性算子 $\Phi^{(m)}(\theta)$ 以前的记号, 我们有

$$\Phi^{(m)}(\theta): z_m \mapsto z'_m = e^{im\theta} z_m.$$

这种所谓的群 SO(2) 的一维酉表示 $\Phi^{(m)}: \Phi_\theta \mapsto e^{im\theta}, m \in \mathbb{Z}$, 在分析中扮演着重要的角色.

我们看到, 作用 Φ 诱导群 SO(2) 在整个空间 V_m 上的一个作用, 从这一角度看, H_m 是 V_m 的一个不变子空间.

问题 2 对可能出现的有机化合物的个数的估计, 例如, 化学中环状碳氢化合物的数量, 可归结为下面日常生活中的一个抽象问题: 由 q 个不同颜色的无穷多个珍珠中可以制作多少个不同的长为 n 的项链?

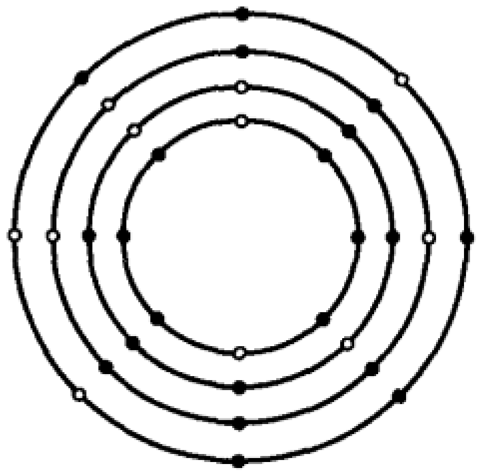


图 4

让我们来试图 (步 G. Polia 的后尘) 来回答这个问题, 如果我们认为项链是有方向的, 那么倒置后的项链一般讲被认为与原先的不同.

我们注意到由 n 个珍珠穿成的串一般有 q^n 种样式 (具有 q 个生成元的自由群中长为 n 的字的个数). 在每一串上循环排列的珍珠可作为具有生成元 $\sigma = (12\cdots n) \in S_n$ 的 n 阶循环群作用在这些串的集合 Ω_n 上. 将这些串的 $\langle\sigma\rangle$ 轨道自然地看成为一个项链, 或者, 也可以这么说, 是某一个同心圆的集合 (图 4). 这第二种解释更明了. 这个群与一个同构相联系

$$\Phi: \sigma \mapsto \Phi(\sigma) = \begin{pmatrix} \cos\dfrac{2\pi}{n} & -\sin\dfrac{2\pi}{n} \\ \sin\dfrac{2\pi}{n} & \cos\dfrac{2\pi}{n} \end{pmatrix},$$

这个同构我们在前面已经遇到过, 它在后面将被称为群 $\langle\sigma\rangle$ 的 2 维线性实表示. 所求的项链的个数 r 由第 1 章 §3 习题 8 中的公式表达. 如果 $d|n$, 那么阶为 n/d 的元 σ^d 保持那种的线段 (和项链) 不动, 这些线段由长为 n/d 的 d 个周期组成 (参见 [BA I] 第 4 章 §2 习题 12, 13). 因此 $N(\sigma^d) = q^d$, 而 $N(\sigma^k) = q^m$, 其中 $m = \text{g.c.d}(n, k)$

为 n 与 k 的最大公因子. $\varphi(n/d)$ 个被加数 (这里 φ 是一个欧拉函数) 恰好与和式 $\sum_k N(\sigma^k)$ 中满足 $\text{g.c.d}(n,k)=d$ 的值 $N(\sigma^k)$ 一致. 于是

$$r=\frac{1}{n}\sum_{d|n}\varphi\left(\frac{n}{d}\right)q^d. \tag{**}$$

借助于通常的二面体群 D_n 的二维线性表示, 使得转动这些不同的 (标定方向的) 项链与 Ω_n 中其余元素 (看作相同) 相关. 试想办法独立地做这些.

不仅在以上所考虑的例子中, 而且在现实的物理问题中, 群的线性表示作为对称的反映自然而然地出现. 相应地, 表示论的思想和语言是非常自然的. 比如 §1 中所举的例子就关系到一些人所共知的问题, 似乎并没有什么新的东西. 同时, 它们同出现在 "一个屋檐下" 的事实本身也会使人产生一些有益的联想.

研究群表示有双重目的: 1) 纯粹数学目的, 多多少少地希望利用补充方法来研究群本身; 2) 应用目的, 譬如说, 群表示在晶体学和量子化学中有明显的贡献. 这两方面实际上都没有反映在本章. 本章的目的很简单, 就是通过我们易懂的线性代数和群论基础来讲讲群表示的一些基本内容.

§1 线性表示的定义和例子

1. 基本概念 严格地说, 当我们在第 1 章 §2 介绍群在集合上的作用时, 我们已经讲了群表示. 现在我们取域 K 上的 n 维向量空间 V 作为一个集合并且在所有 $V\to V$ 的双射变换群 $S(V)$ 中选取一个子群 $\mathrm{GL}(V)$, 它是 V 上可逆线性算子群 (即向量空间 V 的自同构群). 显然, 对于 V 的任意一组基 $(e_1,\cdots,e_n)$, 群 $\mathrm{GL}(V)$ 在这组基下产生一个通常的矩阵群 $\mathrm{GL}(n,K)$, 它可以被认为是线性空间 K^n 的自同构群. 在这种情况下, 每个线性算子 $\mathcal{A}\in\mathrm{GL}(V)$ 对应一个矩阵 $A=(a_{ij})$ 满足

$$\mathcal{A}e_j=\sum_{i=1}^n a_{ij}e_i,\ a_{ij}\in K,\ \det\ A\neq 0.$$

定义 1 设 G 是一个群. 任意同态 $\Phi: G\to\mathrm{GL}(V)$ 称为 G 到空间 V 的一个**线性表示**. 一个线性表示称为**忠实的**, 如果表示的核 $\mathrm{Ker}\,\Phi$ 由群 G 的单位元组成; 一个线性表示称为**平凡表示** (或**单位表示**), 如果对于所有 $g\in G, \Phi(g)=\mathcal{E}$ 为单位算子. 维数 $\dim_K V$ 也称为**表示的维数**. 当 $K=\mathbb{Q},\mathbb{R},\mathbb{C}$ 时, 那么, 相应地称为群 G 的**有理表示、实表示和复表示**.

于是, 线性表示实际上是一个由一个**表示空间** V (或称 G–**空间**) 和一个同态 $\Phi: G\to\mathrm{GL}(V)$ 组成的对 (Φ,V). 由定义知

$$\Phi(e)=\mathcal{E}\ \text{为单位算子},$$
$$\Phi(gh)=\Phi(g)\Phi(h),\ \text{对于所有}\ g,h\in G.$$

对于线性算子 $\Phi(g)$ 在向量 $v \in V$ 上的作用, 我们规定一个记号 $g * v$, 那么按照线性算子的性质, 我们有相应的关系

$$\begin{aligned} &g * (u+v) = g * u + g * v, \quad u, v \in V, \\ &g * (\lambda v) = \lambda(g * v), \qquad \lambda \in K, \\ &e * v = v, \\ &(gh) * v = g * (h * v), \end{aligned} \tag{1}$$

这后面两个等式是上面有关 Φ 的两个等式的另一种表达形式 (对比第 1 章 §3 第 1 目 i), ii)). 在线性表示 (Φ, V) 中关系 (1) 首先突出了 G–空间 V, 出于某种原因, 这样有方便之处 (例如, 当 V 不是抽象的线性空间, 而是某个它的具体实现).

另一方面, 线性空间 V 也许不出现. 如果线性表示可直截了当地解释为群 G 到矩阵群 $\mathrm{GL}(n,k)$ 内的同态 Φ, 我们仍然有 $\Phi_{gh} = \Phi_g\Phi_h$, 但这里的 Φ_g 是一个非退化矩阵, 且 $\Phi_e = E$ 为单位矩阵. 从计算的角度, 线性表示的矩阵解释是更加可以接受的, 但矩阵解释较少不变量且失去了空间的直观性. 然而重要性在于它能自由地运用 (不复杂) 由 G–空间到矩阵以及矩阵到 G–空间的技巧.

关于这种联系, 由线性代数课程 [BA II], 我们知道, 同一个线性变换在不同基下的两个矩阵 A, B 是相似的: $B = CAC^{-1}$ (这里 C 是一个基到另一个基的过渡矩阵). 在表示中, 当我们谈到线性算子群, 对于基的依赖性有如下定义

定义 2 一个群 G 的两个线性表示 $(\Phi, V), (\Psi, W)$ 称为**等价的** (**同构的**或**相似的**), 如果存在一个向量空间的同构 $\sigma: V \to W$, 对于所有的 $g \in G$, 使下图

$$\begin{array}{ccc} V & \xrightarrow{\ \sigma\ } & W \\ {\scriptstyle\Phi(g)}\downarrow & & \downarrow{\scriptstyle\Psi(g)} \\ V & \xrightarrow{\ \sigma\ } & W \end{array}$$

为交换图, 也就是说,

$$\Psi(g)\sigma = \sigma\Phi(g), \quad g \in G,$$

或者, 等价地说

$$\Psi(g) = \sigma\Phi(g)\sigma^{-1} \tag{2}$$

(比较第 1 章 §3 习题 1 中所给出的群在集合上的作用的等价性的定义). 有时我们将两个等价的表示记为 $\Phi \approx \Psi$, 而对于不等价的表示记为 $\Phi \not\approx \Psi$.

我们也给出定义 2 的两个不同的说法.

a) G–**空间的术语**　假设 G 是一个群, $V: (g, v) \mapsto g * v, W: (g, w) \mapsto g \diamond w$ 为具有满足条件 (1) 的作用 $*, \diamond$ 的两个 G–空间. 如果

$$g \diamond \sigma(v) = \sigma(g * v) \tag{2'}$$

对于所有 $g \in G$ 和 $v \in V$ 成立, 那么向量空间的同构 $\sigma : V \to W$ 是 G–空间的同构. 此时也称映射 σ 与 G 作用可交换.

b) **矩阵术语** 如果 $V = \langle v_1, \cdots, v_n \rangle, W = \langle w_1, \cdots, w_n \rangle$ 且 Φ_g, Ψ_g 为线性算子 $\Phi(g), \Psi(g)$ 在相应基下的矩阵, 那么等价于条件 (2) 有下列形式

$$\Psi_g = C\Phi_g C^{-1}, \tag{2''}$$

这里 C 是某一个非退化矩阵, 同样对于所有 $g \in G$. 所有考虑矩阵的系数属于同一个域 K.

(2″) 式所表示的矩阵的相似关系是一个等价关系, 它把 $M_n(K)$ 划分为互不相交的类. 相应的群 G 的表示被分解为等价表示类. 后面可以明显看到, 等价表示类对于表示论是有益的而且是基本的.

我们再将目光转到线性代数教程, 我们希望能更直观地表示群在空间 V 上的作用 $\Phi(G)$. 对于 V 上的线性算子 $\mathcal{A} : V \to V$ 可能存在一个不变子空间$U : u \in U \Longrightarrow \mathcal{A}u \in U$. 将 U 的任一基 $(e_1, \cdots, e_k)$ 添加向量成为整个向量空间 V 的基 $V = \langle e_1, \cdots, e_k, e_{k+1}, \cdots, e_n \rangle$, 我们看到算子 $\mathcal{A}$ 在基 $(e_1, \cdots, e_n)$ 上的矩阵为具有下列形式的分块三角矩阵

$$A = \begin{pmatrix} A_1 & A_0 \\ 0 & A_2 \end{pmatrix},$$

其中 A_1 对应于不变子空间 U, 而 A_2 对应于商空间 V/U. 如果 A_0 是一个零矩阵, 则 $A = A_1 \dot{+} A_2$ 是两个分块矩阵的直和, 而 $V = U \oplus W$ 是两个不变子空间的直和.

只要域 K 是代数闭域, 那么 $\mathcal{A}$ 的真不变子空间的存在性总是有保障的 (参见 [BA II]). 例如, 如果 $K = \mathbb{C}$, 那么取向量 $v \in V, v \neq 0$, 使 $\mathcal{A}v = \lambda v$, 这里 λ 为矩阵

$$f_{\mathcal{A}}(t) = |tE - A| = t^n - (\mathrm{tr} A)t^{n-1} + \cdots + (-1)^n \det A$$

的特征根 (A 是线性算子 $\mathcal{A}$ 的任一矩阵). 我们可以选取 V 的一组基使 A 有三角形形式:

$$A = \begin{pmatrix} \lambda_1 & & & * \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{pmatrix},$$

其对角线上的元素 $\lambda_1, \lambda_2, \cdots, \lambda_n$ 就是特征根. 一些更为精细的分析可以将 A 化简为**若尔当标准形** $J(A)$ (参见 [BA II]), 即为若尔当块 (它是一个 $m \times m$ 矩阵, λ 是 A 的一个特征根)

$$J_{m,\lambda} = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & \lambda \end{pmatrix},$$

的直和.

如果 $A^q=E$, 那么对于矩阵 A 的每个若尔当块 $J_{m,\lambda}$, 我们有 $J_{m,\lambda}^q=E$ 为一个 $m\times m$ 单位矩阵, 显然, 这只能是 $m=1$ 且 λ 为 1 的 q 次方根 (前面假设了 $K=\mathbb{C}$). 这表明, 对于某一可逆矩阵 C

$$A^q=E\Longrightarrow CAC^{-1}=\begin{pmatrix}\lambda_1 & & & 0\\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n\end{pmatrix},\quad \lambda_i^q=1. \tag{3}$$

而这本身也可以由更简单的可对角化的判别准则得到: 当一个线性算子 $\mathcal{A}$ 有一个矩阵 A 和无重根的特征多项式 $f_A(t)=t^q-1$, 则 $\mathcal{A}$ 可对角化.

在转到线性算子群 $\{\Phi(g)|g\in G\}$ 时, 对于个别线性算子 $\mathcal{A}:V\to V$ 的考虑是有益的.

定义 3 设 (Φ,V) 为群 G 的线性表示. 子空间 $U\subset V$ 称为对 G**不变的** (或对 G**稳定的**), 如果对于所有 $u\in U$ 和所有 $g\in G$, 我们有 $\Phi(g)u\in U$. 零子空间和 V 本身是平凡的 G 不变子空间. 只有平凡不变子空间的表示称为**不可约的**. 一个至少有一个非平凡的不变子空间的表示称为**可约的**.

按上面所说, 当表示 (Φ,V) 可约且 V 有不变子空间 U 时, 空间 V 有一组基, 在此基下, 对于所有 $g\in G$, 有一个相关的矩阵

$$\Phi_g=\begin{pmatrix}\Phi'_g & \Phi^0_g\\ 0 & \Phi''_g\end{pmatrix}. \tag{4}$$

因为 $\Phi'_{gh}=\Phi'_g\Phi'_h, \Phi'_e=E_k$ 且 $\Phi'_g(U)\subset U$, 所以映射 $\Phi':g\mapsto\Phi'_g$ 定义了 U 上的一个表示, 称之为 Φ 的**子表示**. 同样可以在商空间 V/U 上定义表示. 它称为**商表示**, 并对应于矩阵 $\Phi''_g, g\in G$.

如果在 V 中可以选择基使得 (4) 中的所有矩阵 Φ^0_g 为零, 那么就称表示 Φ 可分且 $\Phi=\Phi'+\Phi''$ 为直和. (Φ,V) 能分解为直和只有当不变子空间 $U\subset V$ 有一个补不变子空间 W 满足 $V=U\oplus W$ 为子空间的直和且 $\Phi(U)\subset U,\Phi(W)\subset W$. 在这种情形下, $\Phi'=\Phi|_U, \Phi''=\Phi|_W$ 分别为 Φ 在 U 和 W 上的限制.

线性表示 (Φ,V) 称为**不可分的**, 如果它不能表示为两个非平凡子表示的直和. 同样地, 可定义**不可分** G–**空间** V.

如果可能, 将 V,U,W 等继续进行这种不变子空间的直和分解, 最后我们得到 V 的一个不变子空间的直和 $V=V_1\oplus\cdots\oplus V_r$ (相应地有一个表示的直和$\Phi=$

$\Phi^{(1)}\dot{+}\cdots\dot{+}\Phi^{(r)}$). 这时适当选择 V 的一个基, 那么线性算子的矩阵取如下形式.

$$\Phi_g = \begin{pmatrix} \Phi_g^{(1)} & 0 & \cdots & 0 \\ 0 & \Phi_g^{(2)} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \Phi_g^{(r)} \end{pmatrix}.$$

定义 4 *群 G 的线性表示 (Φ, V) 称为完全可约的, 如果它是不可约表示的直和. 类似的术语可应用于 G–空间.*

从线性表示的建立过程可以直观地看到, 不可约表示扮演着构造块的角色. 完全可约表示可由最简单的结构 —— 直和而得到. 下面我们将看到, 对于描写所有表示, 在很多情况下, 这已经足够了. 我们指出, 某些物理上重要的群, 如洛伦兹群, 有无穷维不可约表示. 自然地, 它们绝对不会简化为有限维的, 因此需要单独研究.

2. 线性表示的例子 我们已经引入了表示理论的所有重要的概念. 现在我们需要充实它的实际内容, 为此首先介绍 (并有根据地弄明白) 一系列可约的例子是十分有益的.

例 1 域 K 上的一般线性群 $\mathrm{GL}(n, K)$, 由定义, 有一个 n 维的忠实不可约线性表示, 其表示空间 $V = K^n$. 任意线性群 $H \subset \mathrm{GL}(n, K)$ 都作用在这个空间上, 但可能是可约的.

类似地讨论在第 1 章 §1 见到的其它典型群. 譬如说, 酉群 $\mathrm{U}(n)$ 不可约地作用在埃尔米特空间上, 而正交群 $\mathrm{O}(n)$ 不可约地作用在欧几里得空间上. 这可以直接由 [BA II] 中所证明过的更一般的断言得到. 此断言是, 群 $\mathrm{U}(n)$ 和 $\mathrm{O}(n)$ 可以可迁地作用 (在第 1 章 §3 第 3 目的例 3 的意义下) 在单位长的向量集合上.

例 2 令 $\mathrm{GL}(n, K)$ 按规则 $\Psi_A : X \to AX$ ($A \in \mathrm{GL}(n, K), X \in M_n(K)$) 作用在 n 阶矩阵的向量空间 $M_n(K)$ 上. 不难验证, $\Psi_A(\alpha X + \beta Y) = \alpha\Psi_A(X) + \beta\Psi_A(Y), \Psi_{AB} = \Psi_A\Psi_B$. 因此 $(\Psi, M_n(K))$ 是 n^2 维的线性表示. 令 $M_n^{(i)}$ 是具有唯一非零列 $X^{(i)}$ 的矩阵

$$\begin{pmatrix} 0 & \cdots & x_{1i} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & x_{ni} & \cdots & 0 \end{pmatrix}$$

构成的子空间. 容易验证, 这个子空间是 Ψ_A 不变的. 这里 $A \in \mathrm{GL}(n, K)$, 且在 $\mathrm{GL}(n, K)$ 作用下是不可约的, 并且同构于 (作为 $\mathrm{GL}(n, K)$–空间) 自然空间 K^n. 因此

$$M_n(K) = M_n^{(1)}(K) \oplus \cdots \oplus M_n^{(n)}(K)$$

是 n 个互相同构的 $\mathrm{GL}(n,K)$ 子空间的直和分解, 其对应于 n 个等价表示的直和分解

$$\Psi = \Psi^{(1)}\dot{+}\cdots\dot{+}\Psi^{(n)}.$$

我们也将它们写为

$$M_n(K) \cong nM_n^{(1)}(K), \quad \Psi \approx n\Psi^{(1)}.$$

例 3 现在我们定义群 $\mathrm{GL}(n,K)$ 在 $M_n(K)$ 上的作用 $\Phi, \Phi_A : X \mapsto AXA^{-1}$. 那么 $(\Phi, M_n(K))$ 是 n^2 维的线性表示. 如果 $X = (x_{ij})$, 那么, $\mathrm{tr}X = \sum_{i=1}^{n} x_{ii}$ 为矩阵 X 的迹. 大家知道, $\mathrm{tr}(\alpha X + \beta Y) = \alpha\mathrm{tr}X + \beta\mathrm{tr}Y$ (即 tr 是线性函数) 且 $\mathrm{tr}\Phi_A(X) = \mathrm{tr}X$. 于是, 迹为零的矩阵集合 $M_n^0(K)$ 是一个关于 Φ 不变的子空间. 另一方面, $\Phi_A(\lambda E) = \lambda E$, 且 $\mathrm{tr}\lambda E = n\lambda$. 于是, 当 K 是特征为零的域时, 有 $\mathrm{GL}(n,K)$–子空间的直和分解

$$M_n(K) = \langle E\rangle \oplus M_n^0(K), \tag{5}$$

其直和项的维数分别为 1 维和 n^2-1 维. 当 $n=p$ 且 $K=Z_p$ 时, 形如 (5) 的分解是不存在的, 因为此时 $\mathrm{tr}E = 0$.

根据定义, 矩阵 X 的若尔当标准型 $J(X)$ 不是别的, 正是包含 X 的 $\mathrm{GL}(n,\mathbb{C})$–轨道的某一最简单的表示. 在任一子群 $H \subset \mathrm{GL}(n,K)$ 上的限制自然地产生了有关 H–轨道的有限表示的问题.

例 4 在上面例子中, 令 $K=\mathbb{R}, \Phi$ 为在正交群 $\mathrm{O}(n)$ 上的限制. 因为 $A \in \mathrm{O}(n) \Longleftrightarrow {}^tA = A^{-1}$, 所以 ${}^t(AXA^{-1}) = {}^tA^{-1}\cdot{}^tX\cdot{}^tA = A^tXA^{-1}$. 选择矩阵 $Y + {}^tY$ 或 $Y - {}^tY$ 作为 X, 我们看到, 群 $\mathrm{O}(n)$ 的表示空间 $M_n(\mathbb{R})$ 可以写成 $\mathrm{O}(n)$–子空间的和的形式:

$$M_n(\mathbb{R}) = \langle E\rangle_{\mathbb{R}} \oplus M_n^+(\mathbb{R}) \oplus M_n^-(\mathbb{R})$$

—— 一个由纯量矩阵组成的一维空间 $\langle E\rangle_{\mathbb{R}}$, 一个具有零迹的 $(n+2)(n-1)/2$ 维对称矩阵空间和 $n(n-1)/2$ 维斜对称空间. 大家知道, 对称 (斜对称) 矩阵与对称 (相应地, 斜对称) 双线性型是一一对应的. $\mathrm{O}(n)$ 在 $\langle E\rangle_{\mathbb{R}} \oplus M_n^+(\mathbb{R})$ 和 $M_n^{-1}(\mathbb{R})$ 上的作用也可以转到相应形式的空间上. 二次型 $q(x)$ 变换到主轴的定理不是别的, 正是在包含 $q(x)$ 的 $\mathrm{O}(n)$–轨道中可以选择对角形式 $\sum_i \lambda_i x_i^2$ (其中 λ_i 为实数) 的可能性, 这个对角形式精确到置换是唯一确定的.

用 $\mathbb{C}$ 代替 $\mathbb{R}$ 并用酉群 $\mathrm{U}(n)$ 替代 $\mathrm{O}(n)$, 我们得到一个纯量 $\mathrm{U}(n)$–子空间, 具有零迹的埃尔米特空间和斜埃尔米特空间的直和分解:

$$M_n(\mathbb{C}) = \langle E\rangle_{\mathbb{C}} \oplus M_n^+(\mathbb{C}) \oplus M_n^-(\mathbb{C}).$$

当 $n=2$ 时, 已在第 1 章 §1 中详细讨论过.

例 5 设 G 是作用在某一个具有 $|\Omega| = n > 1$ 个元素的集合 Ω 上的置换群, 即 $G \subset S_n$.

$$V = \langle e_i | i \in \Omega \rangle_K$$

是特征为零的域 K 上的一个向量空间, 其基的元素用 Ω 中元编号. 令

$$\Phi(g)\left(\sum_{i\in\Omega}\lambda_i e_i\right) = \sum_{i\in\Omega}\lambda_i\Phi(g)e_i = \sum_{i\in\Omega}\lambda_i e_{g(i)}$$

($i \mapsto g(i)$ 为 $g \in G$ 在 $i \in G$ 上置换作用). 因为 $(gh)(i) = g(h(i))$, 所以我们得到群 G 的一个 n 维线性表示. 它不会是不可约的, 因为

$$V = \left\langle\sum_{i\in\Omega}e_i\right\rangle \oplus \left\{\sum_{\lambda_1+\cdots+\lambda_n=0}\lambda_i e_i | \lambda_i \in K\right\} \tag{6}$$

是一个一维不变子空间和 $(n-1)$ 维不变子空间的直和分解 (如果 $\operatorname{char} K = p > 0$ 且 $p|n$, 那么直和就得不到). 分两种情形:

a) $G = S_n$. 如果将第 i 个坐标列 $E^{(i)}$ 对应作为 e_i, 则在第 1 章 §4 练习 13 所构造的单射 $S_n \to \mathrm{GL}(n, \mathbb{R})$ 与我们的线性表示 Φ 相同. 分解式 (6) 表明, 对 S_n 存在一个更精练的嵌入 $S_n \to \mathrm{GL}(n-1, Q)$. 晚些时候, 我们将证明这个 $n-1$ 维线性表示的不可约性 (甚至在域 $\mathbb{C}$ 上).

b) 正则表示. 假设 G 是任一有限群. 令 $\Omega = G$, 则我们得到所谓正则的 G–空间 $V = \langle e_g | g \in G \rangle$ 以及相应的群 G 的**正则表示**$(\rho, V) : \rho(a)e_g = e_{ag}$, 对所有 $a, g \in G$. 可以说, 正则表示在某种意义上我们已经接触过, 实际上就是在 [BA I] 第 4 章证明凯莱定理时, 不过那时我们的兴趣不是空间 V, 而是它的基向量的集合 $\{e_g\}$. 正则表示的重要性在于它精确到等价包含 G 的所有不可约表示. (见 §5)

例 6 一维表示是群 G 到域 K 的乘法群 K^* 的一个简单的同态 $\Phi : G \to K^*$ (K 是自身上的一维向量空间). 因为域的乘法群是交换的, 所以 $\operatorname{Ker}\Phi \supset G'$, 这里 G' 是群 G 的换位子群 (第 1 章 §4 定理 5). 我们指出, 两个一维表示 Φ', Φ'' (具有同一个表示空间) 是等价的充要条件是它们相等, 因为

$$a\Phi'(g)a^{-1} = \Phi''(g) \Longrightarrow \Phi'(g) = \Phi''(g) \Longrightarrow \Phi' = \Phi''.$$

设 $g^n = e$, 则 $\Phi(g)^n = \Phi(g^n) = \Phi(e) = 1$, 即 $\Phi(g)$ 是一个单位根. 任意一维表示的核可能是非平凡的, 甚至对于循环群 G. 如果, 例如, $G = Z_4$ 且 $K = Z_{11}$, 则 $\operatorname{Ker}\Phi \supset 2Z_4$. 另一方面, 当 $K = \mathbb{C}$ 时, 任一循环群有忠实的一维表示.

a) $G = (\mathbb{Z}, +)$. 表示 $k \mapsto \lambda^k$ 在 $|\lambda| \neq 1$ 时是忠实的. 如果 $|\lambda| = 1$, 那么由欧拉公式 $\lambda = e^{2\pi i\theta}, \theta \in \mathbb{R}$ 且映射 $k \mapsto e^{2\pi ik}$ 的核仅在 $\theta \in \mathbb{Q}$ 时不等于零.

群 $\mathbb{Z}$ 有任意高维的不可分的复数表示, 然而它们不是不可约的. 这只需引用矩阵的若尔当标准形理论来看映射

$$k \mapsto J_{m,1}^k = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}^k.$$

b) $G = \langle a | a^n = e \rangle$. 令 $\varepsilon = \exp(2\pi i/n)$ 为 1 的 n 次本原根. 对于这个 n, 一维表示

$$\Phi^{(m)} : a^k \mapsto \varepsilon^{mk}, \quad m = 0, 1, \cdots, n-1, \tag{7}$$

正好有 $\varphi(n)$ 个. 我们指出一个有趣的事实: 阶为 n 的循环群在 $\mathbb{C}$ 上有 n 个两两不等价的不可约表示, 它们都是一维的且具有 (7) 的形式.

事实上, 我们仅仅需要验证这样一个事实: 有限循环群在 $\mathbb{C}$ 上没有维数 > 1 的不可约表示. 但是在定义 3 之前我们已经看到了这样的事实: 任意有限阶的线性算子 Φ_g 在 $\mathbb{C}$ 上可对角化. 于是在现在这种情况下, 它等于说表示 Φ 是完全可约的. 如果 $\dim\Phi = r$, 那么 Φ 分解为 r 个一维表示的直和.

实际上, 对于有限阶的循环群, 我们得到了所有复线性表示的描写. 精确到等价,

$$\Phi_g = \begin{pmatrix} \Phi_g^{(i_1)} & & 0 \\ & \ddots & \\ 0 & & \Phi_g^{(i_r)} \end{pmatrix},$$

其中 $\Phi^{(m)}$ 是形如 (7) 的表示之一.

我们的目的是弄清楚在一般情况下的相似的规律性.

例 7 在前面的例子中我们已经觉察到群 G 的线性表示 Φ 的性质对于域 K 有很大的依赖性. 所以, 对于这个问题需要另外说明.

阶为素数 p 的循环群 $G = \langle a | a^p = e \rangle$ 按照规则 $a * v_1 = v_1, a * v_2 = v_1 + v_2$, 作用在特征为 p 的任意域 K 上的 2 维向量空间 $V = \langle v_1, v_2 \rangle$ 上, 则它定义了一个不可分的表示 (Φ, V):

$$a^k \mapsto \Phi_a^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}, 0 \leqslant k \leqslant p-1.$$

事实上, 矩阵 Φ_a 有 2 重特征根 1. 于是若 Φ 能分解为两个一维表示的直和, 这意味着存在一个可逆矩阵 C 使得 $C\Phi_a C^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, 从而 $\Phi_a = C^{-1}EC = E$, 这是不可能的.

下面令 $G = \langle a | a^3 = e\rangle$ 是一个 3 阶循环群且 $K = \mathbb{R}, V = \langle v_1, v_2\rangle$. 那么由该基上的矩阵

$$\Phi_a = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$$

所确定的二维表示 (Φ, V) 不可约, 这因为这个矩阵的特征多项式 $t^3 + t + 1$ 没有实根. 但如果 V 看成是 $\mathbb{C}$ 上的向量空间, 那么, 自然地, V 可以分解为一维 G–子空间的直和

$$V = \langle v_1 + \varepsilon^{-1} v_2\rangle \oplus \langle v_1 + \varepsilon v_2\rangle$$

且

$$C\Phi_a C^{-1} = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}, \quad \varepsilon = \frac{-1+\sqrt{3}}{2}, \quad C = \begin{pmatrix} 1 & -\varepsilon^{-1} \\ 1 & -\varepsilon \end{pmatrix}.$$

于是, 表示的不可约性质在扩域上可能消失.

今后, 除少数情况外, 基域 K 将是复数域 (从实际角度看最重要) 或特征为零的任意代数闭域.

习 题

1. 群 SO(2) 所具有的自然的二维表示

$$\Phi'(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

在 $\mathbb{R}$ 上不可约. 试验证

$$A\Phi'(\theta)A^{-1} = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$$

其中

$$A = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{C}).$$

这就是说, Φ' 是 $\mathbb{C}$ 上两个不等价的一维表示的直和.

2. 当 $n = 2$ 和 $n = 3$ 时, 在分解式 (5) 中的 $\mathrm{GL}(n, \mathbb{C})$–空间 $M_n^0(\mathbb{C})$ 不可约吗?

3. 假设 Φ 和 Ψ 是 n 阶循环群 $\langle a | a^n = e\rangle$ 的两个不可约复表示. 证明

$$\frac{1}{n}\sum_{k=0}^{n-1} \Phi(a^k)\overline{\psi(a^k)} = \begin{cases} 1, & \text{如果 } \Phi \approx \Psi, \\ 0, & \text{如果 } \Phi \not\approx \Psi. \end{cases}$$

4. 根据习题 3, 证明下列断言的正确性: 有限循环群 $\langle a | a^n = e\rangle$ 上的任一复值函数 f “按初等调和” 可以写为分解式

$$f(a^k) = \sum_{m=0}^{n-1} c_m \varepsilon^{mk}, \quad \varepsilon = \exp\left(\frac{2\pi i}{n}\right).$$

"傅里叶系数" c_m 可以由公式

$$c_m = \frac{1}{n}\sum_{k=0}^{n-1} f(a^k)\varepsilon^{-mk}$$

算出.

5. 利用项链个数的公式 (参见本章开始部分) 推出下列基本结果:

a) $q^p - q \equiv 0 \pmod p$ (费尔马小定理, 见第 4 章 §4);

b) $\sum_{d|n}\varphi(d) = n$.

§2 酉性和可约性

1. 酉表示 回想 (参见 [BA II]) 在线性代数教程中, 复数域 $\mathbb{C}$ 上的向量空间 V 上的非退化形式 $(u,v)\mapsto(u|v)$ 被称为**埃尔米特型**, 如果

$$\begin{aligned}&(u|v) = \overline{(v|u)},\\&((\alpha u+\beta v)|w) = \alpha(u|w)+\beta(v|w),\\&(v|v)>0,\ \text{对所有}\ v\neq 0\end{aligned}\tag{1}$$

(与通常一样, $z\mapsto\bar z$ 是复数共轭自同构). 向量空间 V 与非退化的埃尔特型 $(u|v)$ 一起称为**埃尔米特空间**. 埃尔米特空间在实数域上的类似物就是具有内积的**欧几里得空间**, 其内积由一个非退化的对称双线性型给出.

给定 V 的一个基 $e_1,\cdots,e_n$, 并设 $u=\sum_i u_ie_i, v=\sum_j v_je_j$, 则

$$(u|v) = \sum_{i,j} h_{ij}u_i\overline{v}_j,$$

其中矩阵 $H=(h_{ij})$ 满足条件 $\bar h_{ij} = h_{ji}$, 且 H 也称为埃尔米特矩阵.

存在标准正交基 (即满足条件 $(e_i|e_j)=\delta_{ij}$), 满足

$$(u|v) = \sum_{i=1}^{n} u_i\overline{v}_i.$$

保持这个型, 即 $(\mathcal{A}u|\mathcal{A}v)=(u|v)$ 的线型算子 $\mathcal{A}: V\to V$ 称为酉算子. 在实空间时, 它相应地称为正交算子. 酉算子写为矩阵的形式是 $A\cdot{}^t\bar A = E$, 其中 $A=(a_{ij})$, ${}^t\bar A = A^* = (\bar a_{ji})$, 这些我们已经在第 1 章中见到过了. 如同 [BA II] 中一样, 我们用 $\mathcal{A}^*$ 表示对应于矩阵 $A^* = \overline{{}^tA}$ 的线性算子, 其酉性条件表现为 $\mathcal{A}\cdot\mathcal{A}^* = \varepsilon = \mathcal{A}^*\cdot\mathcal{A}$. 所有酉矩阵的群 (酉算子群或简单地说酉群) 用符号 $\mathrm{U}(n)$ 表示. 根据定义, $\mathrm{U}(n)\subset\mathrm{GL}(n,\mathbb{C})$, 且如果表示 $\Phi: G\to\mathrm{GL}(n,\mathbb{C})$ 满足 $\mathrm{Im}\Phi\subset\mathrm{U}(n)$, 则 (Φ,V) 称为酉表示.

定理 1 有限群 G 在 $\mathbb{C}$ 上的任一线性表示 (Φ,V) 等价于一个酉表示.

证明 在群 G 的表示空间 V 中选择一个非退化的埃尔米特型

$$H:(u,v)\mapsto H(u,v)=\sum_{i,j}h_{ij}u_i\bar{v}_j$$

(记向量空间 V 的某个基为 $(f_1,\cdots,f_n)$), 并考察由 $H(u,v)$ 关于 G "取平均值" 所得的 $(u|v)$:

$$(u|v)=|G|^{-1}\sum_{g\in G}H(\Phi(g)u,\Phi(g)v). \tag{2}$$

乘数 $|G|^{-1}$ 并不重要, 放置它只是为了在 Φ 为酉性的情形时有等式 $(u|v)=H(u|v)$. 因为

$$\begin{aligned}
H(\Phi(g)u,\Phi(g)v)&=\overline{H(\Phi(g)v,\Phi(g)u)},\\
H(\Phi(g)(\alpha u+\beta v),\Phi(g)w)&=H(\alpha\Phi(g)u+\beta\Phi(g)v,\Phi(g)w)\\
&=\alpha H(\Phi(g)u,\Phi(g)w)+\beta H(\Phi(g)v,\Phi(g)w),\\
H(\Phi(g)v,\Phi(g)v)&>0,\quad \text{对于 } v\neq 0 \text{ 和所有} g\in G,
\end{aligned}$$

所以 (2) 式满足条件 (1), 从而是一个非退化的埃尔米特型.

此外 (也是最重要的),

$$\begin{aligned}
(\Phi(h)u|\Phi(h)v)&=\frac{1}{|G|}\sum_{g\in G}H(\Phi(g)\Phi(h)u,\Phi(g)\Phi(h)v)\\
&=\frac{1}{|G|}\sum_{g\in G}H(\Phi(gh)u,\Phi(gh)v)=\frac{1}{|G|}\sum_{t\in G}H(\Phi(t)u,\Phi(t)v)\\
&=(u|v),
\end{aligned}$$

这表明, 对于任意 $g\in G$, 算子 $\Phi(g)$ 保持 $(u|v)$ 不变. 在 V 中选取关于型 $(u|v)$ 的标准正交基. 那么在这个基下由算子 $\Phi(g)$ 所对应的矩阵 Φ_g 将是一个酉矩阵. □

注 1 定理 1 的论断不能由我们所熟悉的事实自动推出这样的结论: 每个具有 $g^m=e$ 的可分矩阵 Φ_g 相似于一个酉对角阵 $\operatorname{diag}(\lambda_1,\cdots,\lambda_n)$, 其中 $\lambda_i^m=1$.

注 2 在实数域的情形, 完全类似的论述可以证明: 表示 (Φ,V) 等价于一个正交表示.

注 3 许多根据表明, 酉表示在表示理论的应用中扮演着重要的角色, 特别值得注意的是, 定理 1 对于更广的紧群类, 如 $\mathrm{U}(n),\mathrm{O}(n)$ 仍然成立. 其证明也一样. 但是群元素的求和需用在群上 (关于某一度量) 的积分法代替. 回想, 紧群 $\mathrm{SU}(2)$ 在几何上与三维球 S^3 分不开, 因此, 例如谈论它的体积是有意义的. 一般地说, 有限群的表示理论和紧群的表示理论有较大的平行现象, 但是我们不可能在此停留. 由 §1 例 6 a) 可见, 非紧群 (例如, $G=\mathbb{Z}$) 的表示不一定是酉的.

最后, 我们指出, 虽然定理 1 的证明是构造性的, 但是运用它去寻找现有表示的酉实现并不太实用. 例如, 对于由元素 $a_1, \cdots, a_d$ 生成的群 G, 只需获得矩阵 $\Phi_{a_1}, \cdots, \Phi_{a_d}$ 的酉性, 那么群 $\Phi(G)$ 就是酉的.

例 1 对称群 $S_3 = \langle (1\ 2), (1\ 2\ 3) \rangle$ 有一个二维表示 Φ, 它作为一个直和项包含在一个自然的三维表示中 (参见 §1 例 5). 即, 如果

$$\Phi(\pi)e_i = e_{\pi i}, \quad i = 1, 2, 3, \quad f_1 = e_1 - e_3, \quad f_2 = e_2 - e_3,$$

那么

$$\begin{aligned} \Phi((1\ 2))f_1 &= e_2 - e_3 = f_2, \\ \Phi((1\ 2))f_2 &= e_1 - e_3 = f_1, \\ \Phi((1\ 2\ 3))f_1 &= e_2 - e_1 = -f_1 + f_2, \\ \Phi((1\ 2\ 3))f_2 &= e_3 - e_1 = -f_1. \end{aligned}$$

因为 $\pi = (1\ 2\ 3)^i(1\ 2)^j$, 其中 $i = 0, 1$ 或 $2, j = 0$ 或 1, 所以不难得到所有的矩阵 $\Psi_\pi = \Phi(\pi)|_{\langle f_1, f_2 \rangle}$:

$$\begin{gathered} e_1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad (1\ 2) \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad (1\ 3) \mapsto \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, \\ (2\ 3) \mapsto \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, \quad (1\ 2\ 3) \mapsto \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad (1\ 3\ 2) \mapsto \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}. \end{gathered}$$

由于 $\det \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} = 1$ 且 $(1\ 2\ 3)^3 = e$, 一定存在某一非退化矩阵 C, 使得

$$C \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} C^{-1} = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}, \quad \varepsilon = \frac{-1 + \sqrt{-3}}{2}.$$

用矩阵 C 作共轭不会改变矩阵 $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ 的酉性. 矩阵

$$C = \begin{pmatrix} 1 & -\varepsilon^2 \\ -\varepsilon^2 & 1 \end{pmatrix}$$

满足线性条件

$$C \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} C, \quad C \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix} C.$$

至此我们有可能来描写我们所熟悉的群 S_3 的酉表示, 这就是单位表示 $\Phi^{(1)}$, $\Phi^{(2)}: \pi \mapsto \operatorname{sgn}(\pi) = \pm 1$ 和刚刚得到的二维表示 $\Phi^{(3)} \approx \Psi$. 为了后面引用方便我们列出下表:

S_3	e	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
$\Phi^{(1)}$	1	1	1	1	1	1
$\Phi^{(2)}$	1	−1	−1	−1	1	1
$\Phi^{(3)}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$	$\begin{pmatrix}0&\varepsilon\\\varepsilon^{-1}&0\end{pmatrix}$	$\begin{pmatrix}0&\varepsilon^{-1}\\\varepsilon&0\end{pmatrix}$	$\begin{pmatrix}\varepsilon&0\\0&\varepsilon^{-1}\end{pmatrix}$	$\begin{pmatrix}\varepsilon^{-1}&0\\0&\varepsilon\end{pmatrix}$

例 2 在第 1 章 §1 所构造的满同态 $\Phi:\mathrm{SU}(2)\to\mathrm{SO}(3)$ 提供了无限群 (也就是 $\mathrm{SU}(2)$) 的自然正交表示.

2. 完全可约性 由 §1 中的定义和注, 显然下列结论是十分重要的.

定理 2 (Maschke 定理) *设 G 是一个有限群, K 是一个域且 K 的特征不整除 $|G|$ (特别地, K 的特征为 0). 则群 G 在 K 上的每个线性表示完全可约.*

定理 2 的断言表明 (Φ,V) 可以分解为不可约表示的直和. 实际上, 经典的 Maschke 定理的内容是下面的.

(M) *每个 G–不变子空间 $U\subset V$ 有一个 G–不变补 W*

$$V=U\oplus W. \tag{3}$$

我们将证明这个结论, 从而定理 2 将由此自动推得. 事实上, 表示 (Φ,V) 要么不可约, 要么存在一个真 G–不变子空间 U. 如果 (Φ,V) 不可约, 则结论自然成立; 如果它有一个真 G–不变子空间 U, 并且有一个 G–子空间 W 使分解式 (3) 成立. 那么在这种情况下, $\dim U<\dim V,\dim W<\dim V$. 对 U 和 W 继续这种推理并按照维数进行归纳, 我们得到具有不可约分量的所要求的分解.

下面我们就来证明结论 (M). 我们首先更感兴趣域 $K=\mathbb{C}$ 的情形, 我们讲述两种独立的证明方法.

第一种证明 ($K=\mathbb{C}$). 依据定理 1, 存在表示空间 V 上的对于线性算子 $\Phi(g)$ 不变的非退化埃尔米特型 $(u|v)$. 对于每个子空间 $U\subset V$ 存在一个*正交补*.

$$U^\perp=\{v\in V|(u|v)=0,\quad \forall u\in U\},$$

按照线性代数课程中熟悉的定理

$$V=U\oplus U^\perp,$$

且 $(U^\perp)^\perp=U$. 现在假设 U 是 V 的一个 G–子空间, 即对所有 $g\in G$, 有 $\Phi(g)U\subset U$. 因为 $\Phi(g)|_U$ 是 U 的一个自同构, 所以任意元 $u\in U$ 可以写成形式 $u=\Phi(g)u',u'\in U$. 利用型的不变性, 我们有

$$v\in U^\perp\Longrightarrow(u|\Phi(g)v)=(\Phi(g)u'|\Phi(g)v)=(u'|v)=0.$$

于是, $v \in U^{\perp} \Longrightarrow \Phi(g)v \in U^{\perp}$. 令 $W = U^{\perp}$, 则得到分解式 (3). □

第二种证明. 与前面一样, 令 U 为 V 中 G 作用不变的子空间. 我们考虑直和

$$V = U \oplus U',$$

其中 U' 为 U 的任一补空间. 一般情况下, U' 不是 G–不变的. 我们来看投射算子 $\mathcal{P}: V \to U'$, 对于任意向量 $v = u + u'$, 定义 $\mathcal{P}v = u'$. 那么

$$v - \mathcal{P}v \in U, \mathcal{P}(U) = 0, \quad \mathcal{P}^2 = \mathcal{P}. \tag{4}$$

现在我们引入 "平均" 线性算子

$$\mathcal{P}_G = |G|^{-1} \sum_{h \in G} \Phi(h)\mathcal{P}\Phi(h^{-1})$$

(因为由条件 K 的特征不整除 $|G|$, 所以用 $|G|$ 除是可以的). 我们断言

$$\Phi(g)\mathcal{P}_G = \mathcal{P}_G\Phi(g), \quad \forall g \in G. \tag{5}$$

事实上,

$$\begin{aligned}\Phi(g)\mathcal{P}_G\Phi(g^{-1}) &= |G|^{-1} \sum_{h \in G} \Phi(g)\Phi(h)\mathcal{P}\Phi(h^{-1})\Phi(g^{-1}) \\ &= |G|^{-1} \sum_{h \in G} \Phi(gh)\mathcal{P}\Phi((gh)^{-1}) \\ &= |G|^{-1} \sum_{t \in G} \Phi(t)\mathcal{P}\Phi(t^{-1}) = \mathcal{P}_G,\end{aligned}$$

于是断言 (5) 成立. 令

$$W = \mathcal{P}_G(V) = \{\mathcal{P}_G v | v \in V\}.$$

由 (5)

$$\Phi(w) = \Phi(g)\mathcal{P}_G v = \mathcal{P}_G\Phi(g)v = \mathcal{P}_G v' = w' \in W$$

对于任意 $w \in W$ 成立. 于是向量子空间 $W \subset V$ 确是一个 G–子空间.

下面只需证明 $V = U \oplus W$ 是 G–子空间的直和. 因为 $\Phi(h^{-1})v - \mathcal{P}\Phi(h^{-1})v \in U$ (见 (4)), 所以

$$v - \Phi(h)\mathcal{P}(h^{-1})v = \Phi(h)\{\Phi(h^{-1})v - \mathcal{P}\Phi(h^{-1})v\} \in \Phi(h)U = U$$

(由 U 的不变性). 于是

$$v - \mathcal{P}_G v = |G|^{-1} \sum_{h \in G} \{v - \Phi(h)\mathcal{P}\Phi(h^{-1})v\} = u \in U,$$

从而我们得到 $v = u + w$, 其中 $w = \mathcal{P}_G v \in W$, 即 $V = U + W$.

又

$$\Phi(h^{-1})U \subset U \Longrightarrow \mathcal{P}\Phi(h^{-1})U = 0 \quad (\text{见 } (4))$$
$$\Longrightarrow \Phi(h)\mathcal{P}\Phi(h^{-1})U = 0 \Longrightarrow \mathcal{P}_G(U) = 0.$$

可见

$$v - \mathcal{P}_G v = u \in U \Longrightarrow \mathcal{P}_G(v - \mathcal{P}_G v) = 0,$$

于是对所有 $v \in V$ 有 $\mathcal{P}_G v = \mathcal{P}_G^2 v$. 这表明 $\mathcal{P}_G$ 是顺着 U 在 W 上的投射:

$$\mathcal{P}_G U = 0, \quad \mathcal{P}_G^2 = \mathcal{P}_G. \tag{6}$$

现在有 $v \in U \cap W \Longrightarrow \mathcal{P}_G v = 0$, 这因为 $v \in U$, 且 $v = \mathcal{P}_G v'$, 这因为 $v \in \mathcal{P}_G(V) = W$. 于是由 (6) 我们得到

$$0 = \mathcal{P}_G v = \mathcal{P}_G(\mathcal{P}_G v') = \mathcal{P}_G^2 v' = \mathcal{P}_G v' \Longrightarrow U \cap W = 0. \qquad \square$$

如果我们不小心会做出更强的断言, 认为分解式中

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$$

的不可约分量 (不可约 G–子空间) 是唯一的. 但, 如果, 例如, $\Phi(g) = \mathcal{E}$ 为单位算子, 对于所有 $g \in G$, 那么 V 的任意一维子空间的直和分解都将是不可约分量的分解, 而这样的分解有无限多个. 另一个问题, 如果我们将所有同构的不可约分量分组:

$$V = U_1 \oplus \cdots \oplus U_s.$$

因为我们不区分同构的 G–空间, 所以可以认为

$$U_1 = V_1 \oplus V_1 \oplus \cdots \oplus V_1 = n_1 V_1,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$U_s = V_s \oplus V_s \oplus \cdots \oplus V_s = n_s V_s,$$

这里 n_i 是 V_i 在 V 的分解式中不可约分量 V_i 出现的重数. 我们看到, 重数是唯一的.

习　题

1. 群 $(\mathbb{R}, +)$ 的任意一维连续表示 (当邻近的算子对应到邻近的数时) 有形式 $\Phi^{(\alpha)} : t \mapsto e^{i\alpha t}$, 这里 α 是一个复数. 证明: $\Phi^{(\alpha)}$ 是酉的当且仅当 $\alpha \in \mathbb{R}$.

2. 群 $(\mathbb{R},+)$ 到 SO(2) 的同态 $f: t \mapsto \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$ 的核由这样的数 $t = 2\pi m, m \in \mathbb{Z}$, 组成. 于是 $\mathrm{SO}(2) \cong \mathbb{R}/(2\pi\mathbb{Z})$, 且群 $\mathbb{R}$ 的不可约酉表示

$$\widetilde{\Phi}: t + 2\pi m \mapsto \Phi(t), \quad 0 \leqslant t \leqslant 2\pi$$

与群 SO(2) 的每个不可约酉表示 (根据 §4 的结果, 它一定是一维的) Φ 相对应, 且 $\widetilde{\Phi}(2\pi) = \Phi(0) = 1$. 由习题 1, 有 $\widetilde{\Phi} = \Phi^{(n)}, n \in \mathbb{Z}$. 结合第 1 目注 3, 这表明群 SO(2) 的任意不可约表示有形式 $\Phi^{(n)}(t) = e^{int}, n \in \mathbb{Z}$. 试证

$$\frac{1}{2\pi}\int_0^{2\pi} e^{ikt} \cdot \overline{e^{ilt}} dt = \delta^{kl}.$$

(与 §1 习题 3 比较: 阶 n 替代群 SO(2) 的数量 2π). 在分析中, 函数系 $\{e^{int}\}$ 当作周期函数 (或圆周 $S' \sim \mathrm{SO}(2)$ 上的函数; 参见 [BA II]) 的完全标准正交系的经典例子. 由此开始了内容丰富的傅里叶级数的理论.

3. 利用 Maschke 定理证明: 非交换有限群的任一忠实复 2 维表示不可约.

§3 有限旋转群

从古到今, 具有丰富对称性的客体一直引起科学家们的注意. 这种对称性客体的最熟悉和最突出的例子是著名的 5 个柏拉图多面体, 这些多面体的美, 人们直接感觉得到. 在各个时代, 这种美都激励着哲学家、数学家、天文学家、物理学家去创建或是神秘或是科学的体系, 这些体系就其严整性与完善性来说, 在美学上符合于正多面体. 1968 年出版了由 20 世纪伟大数学家外尔 (Weyl. H) 有关 "对称" 的一系列讲稿的俄文译本. 此书阐明了在所有科学世界观, 尤其是数学世界观的形成中对称性诸方面研究的重要性. 通过普及性的小册子足以清楚地探察对称性客体数学描写的相互补充的两个方面: 寻找存在的必要条件 (最简单的情形, 对于基本参数立出一个或几个丢番图方程 (见下面 (1)); 和当建立了实际存在的对象显式时的几何作图的问题 (下面有柏拉图多面体的描写). 在群论和群的表示理论的发展过程中, 有关对称的谱的研究变得特别广泛, 它涉及数学、物理、化学、生物以及其它学科的各种不同的领域.

这一节事关群 SO(3) 的有限子群. 掌握它们, 我们同样得到诸如 A_4, S_4, A_5 等群的正交不可约表示, 而且易于记住几何外貌. 一开始读它们时可以放过第 1 目和定理 2 的证明 (很简单), 但是对于那些要检验一下自己掌握 "群作用" 的牢固性的人来说, 熟悉此节的所有内容将是有益的.

1. SO(3) **中有限子群的阶**　根据线性代数课程 [BA II] 中欧拉定理, 任意元 $\mathcal{A} \in \mathrm{SO}(3), \mathcal{A} \neq \mathcal{E}$, 是欧几里得空间 $\mathbb{R}^3$ 中绕某一轴的一个旋转. 换句话说, 在一个二维球面 S^2 上恰好有两个点, 在 $\mathcal{A}$ 作用下不动: 即球面和旋转轴的交点. 这两个点称为旋转 $\mathcal{A}$ 的极点.

现在假设 G 是 SO(3) 中一个有限子群, S 是 G 中所有非单位旋转的极点的集合. 显然, 群 G 作为一个置换群作用在集合 S 上. 如果 x 是某一个旋转 $\mathcal{A} \neq \mathcal{E}, \mathcal{A} \in G$, 的极点, 那么对于任意 $\mathcal{B}$ 有

$$(\mathcal{B}\mathcal{A}\mathcal{B}^{-1})\mathcal{B}x = \mathcal{B} \cdot \mathcal{A}x = \mathcal{B}x,$$

即 $\mathcal{B}x$ 是 $\mathcal{B}\mathcal{A}\mathcal{B}^{-1}$ 的一个极点, 于是 $\mathcal{B}x \in S$. 我们用 Ω 表示有序元素对 $(\mathcal{A}, x)$ 的集合, 其中 $\mathcal{A} \in G, \mathcal{A} \neq \mathcal{E}, x$ 是 $\mathcal{A}$ 的极点. 再假设 G_x 是点 x 的稳定子群 (稳定化子), 即 G 中保持 x 不变的所有元构成的子群. 如果

$$G = G_x \cup g_2 G_x \cup \cdots \cup g_{m_x} G_x$$

为 G 关于 G_x 的左陪集分解, 那么点 x 的 G–轨道将是集合

$$G(x) = \{x, g_2 x, \cdots, g_{m_x} x\},$$

其中元素个数 $|G(x)| = m_x$. 由拉格朗日定理 $N = m_x n_x$, 其中 $N = |G|, n_x = |G_x|$ (与第 1 章 §3 比较, 符号有些变化). 我们指出, n_x 是 G 的这样一个循环子群的阶, 它中的每个元素是围绕过点 x 的轴的旋转. 称 n_x 为**极点 x 的重数**或称 x 是 n_x–极点.

因为 G 中每个元 $\mathcal{A} \neq \mathcal{E}$ 对应两个极点, 所以 $|\Omega| = 2(N-1)$. 另一方面, 对于每个极点 x 有不同于 e 且保持极点 x 不动的 $n_x - 1$ 个 G 中元. 于是, 元素对 $(\mathcal{A}, x)$ 的个数等于下列和

$$|\Omega| = \sum_{x \in s} (n_x - 1).$$

取 $\{x_1, \cdots, x_k\}$ 为按每个轨道中取一个极点的极点的集合, 令 $n_i := n_{x_i}, m_i := m_{x_i}$, 且注意到对于所有 $x \in G(x_i)$, 有 $n_x = n_{x_i} = n_i$, 则我们得到

$$|\Omega| = \sum_{x \in s} (n_x - 1) = \sum_{i=1}^{k} m_i (n_i - 1) = \sum_{i=1}^{k} (N - m_i).$$

于是

$$2N - 2 = \sum_{i=1}^{k} (N - m_i).$$

将 N 分成相等的两部分, 我们有

$$2 - \frac{2}{N} = \sum_{i=1}^{k} \left(1 - \frac{1}{n_i}\right). \tag{1}$$

假设 $N > 1$, 则 $1 \leqslant 2 - 2/N < 2$. 因为 $n_i \geqslant 2$, 所以 $1/2 \leqslant 1 - \dfrac{1}{n_i} < 1$, 从而 k 应该等于 2 或 3.

情形 1. $k = 2$. 则

$$2 - \frac{2}{N} = \left(1 - \frac{1}{n_1}\right) + \left(1 - \frac{1}{n_2}\right),$$

或等价地

$$2 = \frac{N}{n_1} + \frac{N}{n_2} = m_1 + m_2,$$

由此得到 $m_1 = m_2 = 1, n_1 = n_2 = N$. 可见, G 恰有一个旋转轴且 $G = C_N$ 是一个阶为 N 的循环群.

情形 2. $k = 3$. 假设 $n_1 \leqslant n_2 \leqslant n_3$. 如果 $n_1 \geqslant 3$, 那么我们有

$$\sum_{i=1}^{3}\left(1 - \frac{1}{n_i}\right) \geqslant \sum_{i=1}^{3}\left(1 - \frac{1}{3}\right) = 2,$$

这不可能. 于是 $n_1 = 2$, 从而等式 (1) 可写为形式 $1/2 + 2/N = 1/n_2 + 1/n_3$. 显然, 若 $n_2 \geqslant 4 \Longrightarrow 1/n_2 + 1/n_3 \leqslant 1/2$, 矛盾. 因此 $n_2 = 2$ 或 $n_2 = 3$.

如果 $n_2 = 2$, 那么 $n_3 = N/2 = m$ (即 N 应该是偶数) 且 $m_1 = m_2 = m, m_3 = 2$. 这些条件适合一个二面体群 (见第 1 章 §4 第 5 目例 1). 如果 $n_2 = 3$, 那么 $1/6 + 2/N = 1/n_3$, 从而仅有 3 种可能:

2′) $n_3 = 3, N = 12, m_1 = 6, m_2 = 4, m_3 = 4$;

2″) $n_3 = 4, N = 24, m_1 = 12, m_2 = 8, m_3 = 6$;

2‴) $n_3 = 5, N = 60, m_1 = 30, m_2 = 20, m_3 = 12$.

将上面所有的信息收集于表 1.

表 1

N	轨道数	$\|S\|$	中心化子的阶		
n	2	2	n	n	—
$2m$	3	$2m+2$	2	2	m
12	3	14	2	3	3
24	3	26	2	3	4
60	3	62	2	3	5

于是我们已经证明了下列断言

定理 1 *设 G 是 SO(3) 的一个有限子群, 且 G 不是循环群和二面体群. 那么 G 的阶 N 仅仅有 3 种可能: $N = 12, 24, 60$. 在群 G 上的其它限制包含在表 1 中.*

2. 正多面体群 在 SO(3) 中存在阶为 12, 24, 60 的群, 其证明非常简单. 精确到相似, 在欧几里得空间 $\mathbb{R}^3$ 中共存在 5 个 (从古代就知道) 正凸多面体 (参见图 5): 四面体 Δ_4, 立方体 $\square_6$, 八面体 Δ_8, 十二面体 $\bigstar_{12}$ 和二十面体 Δ_{20}:

如果将正多面体 M 的中心摆放在空间 $\mathbb{R}^3$ 的原点, 那么使 M 与自身重合的 SO(3) 中的旋转形成一个有限子群. 在这种情况下, 产生的不是 5 个, 而只有 3 个不

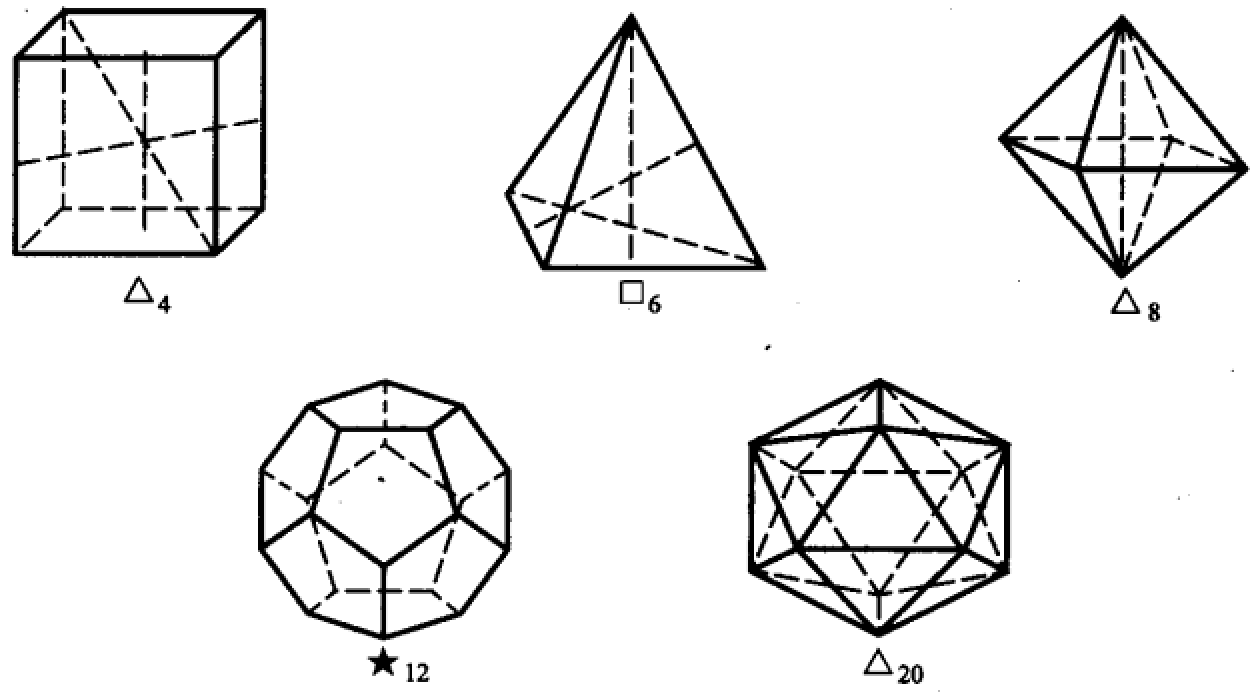


图 5

同的 (不同构的) 旋转群, 这因为对于立方体和八面体, 同样地对于十二面体和二十面体, 其旋转群是相同的. 用几何解释这是非常明显的. 如果将立方体邻面的中心相连接, 那么这些线段将是内接于立方体的八面体的棱边. $\mathbb{R}^3$ 中任意保持立方体不变的旋转就转变为旋转内接八面体, 反之亦然. 对于十二面体和二十面体可以类似地讨论.

在下面表 2 中, N_0 为多面体的顶点的个数, N_1 为棱边的个数, N_2 是多面体的面的个数, μ 是每个面的边 (棱) 的个数, 而 ν 是会聚到同一个顶点的面的个数. 和前面一样, N 为相应的群的阶.

表 2

	N_0	N_1	N_2	μ	ν	N
四面体	4	6	4	3	3	12
立方体	8	12	6	4	3	24
八面体	6	12	8	3	4	24
十二面体	20	30	12	5	3	60
二十面体	12	30	20	3	5	60

根据多面体的欧拉几何定理

$$N_0 - N_1 + N_2 = 2.$$

极点的总数等于

$$N_0 + N_1 + N_2 = 2N_1 + 2.$$

在任一将多面体变为自身的旋转下, 一个给定的棱边将与其它的一个棱边 a_ib_i 或 b_ia_i 重合, 于是 $N = 2N_1$. 我们也看到 $\{\mu, \nu\} = \{n_2, n_3\}$, 这里 n_2, n_3 是在第 1 目中引入的极点的重数.

往下, 令 $\mathbf{T}$ 是四面体群, $\mathbf{O}$ 为立方体群 (八面体群), $\mathbf{I}$ 为二十面体群 (十二面体群).

$\mathbf{T}$ 的元素有围绕连接顶点和对面中心的四个轴的几个角度的旋转, 围绕连接对棱的中心的三个轴之一的 π 角的旋转, 和单位旋转.

在群 $\mathbf{O}$ 中, 除了单位元外, 有围绕连接立方体对面中心的三个轴的角度为 $\pi/2, \pi, 3\pi/2$ 的旋转, 围绕连接极对面顶点的四个轴的角度为 $2\pi/3, 4\pi/3$ 的旋转, 和围绕连接对棱的中心的六个轴中每一个的角度为 π 的旋转.

正四面体内切于立方体, 只有对于 $\mathbf{O}$ 中阶为 3 和 2 的某些旋转不变. 与单位元一起共有 12 个元, 它们正好组成群 $\mathbf{T}$. 于是 $\mathbf{T} \subset \mathbf{O}$, 而因为 $|\mathbf{O} : \mathbf{T}| = 2$, 所以 $\mathbf{T} \lhd \mathbf{O}$.

$\mathbf{O}$ 中的每一个元正好对应于由立方体的四个大对角线组成的集合上的一个置换. 于是由群的阶的相等 $|\mathbf{O}| = |S_4| = 24$ 得出它们的同构: $\mathbf{O} \cong S_4$.

相应地, $\mathbf{T} \cong A_4$.

习题 2 证明了 $\mathbf{I} \cong A_5$.

重新回到定理 1 的证明, 我们看到, 当 $n_1 = 2, n_2 = n_3 = 3$ 时, 有两个极点的四元轨道

$$G(p_1) = \{p_1, p_2, p_3, p_4\},$$
$$G(q_1) = \{q_1, q_2, q_3, q_4\},$$

其中 p_i, q_i 是球面 S^2 上的对径点. 如果 Δ_4^0 是带有顶点 p_i 的四面体, 那么它的对称变换群 $\mathbf{T}^0$ 包含 G. 由 $|G| = 12$ 推出 Δ_4^0 是一个正四面体, 即 $\Delta_4^0 = \Delta_4$ 且 $\mathbf{T}^0 = G = \mathbf{T}$.

当 $n_2 = 3, n_3 = 4$ 时有一个六元极点轨道 $G = (p_1) = \{p_1, p_2, \cdots, p_6\}$, 它们分为对, 因为 $i \neq 3 \Longrightarrow n_i \neq 4$. 这三个球面 S^2 上点对给我们带来八面体 Δ_8^0 的三个对顶点对. 如同前面的情况, $|G| = 24 \Longrightarrow \Delta_8^0$ (就此而言, Δ_8^0 是一个正八面体) 及 $\mathbf{O}^0 = G = \mathbf{O}$.

最后, 当 $n_1 = 2, n_2 = 3, n_3 = 5$ 时建立了具有顶点 p_i 的二十面体 Δ_{20}^0, 这里 p_i 属于轨道 $G(p_i) = \{p_1, \cdots, p_{20}\}$. 又由于 $|G| = 60$, 致使 Δ_{20}^0 是一个正二十面体且有群的相等: $\mathbf{I}^0 = G = \mathbf{I}$. 我们仍然看到, 在球面 S^2 中内切的同一类型的两个正多面体可以通过某种旋转由一个得到另一个 (坐标系的代换). 这形成了 SO(3) 中同构子群的共轭性.

于是我们得到了下列定理的结果.

定理 2 *SO(3) 中所有有限子群精确到同构有且只有*

$$C_n, D_n, \quad n \in \mathbb{N};$$
$$\mathbf{T} \cong A_4, \quad \mathbf{O} \cong S_4, \quad \mathbf{I} \cong A_5.$$

且任意两个同构的有限子群在 SO(3) 中共轭.

推论 定理 2 中的三个同构给出群 A_4, S_4 和 A_5 的不可约三维正交表示.

应用定理 2 和满同态 $\Phi: \mathrm{SU}(2) \to \mathrm{SO}(3)$ (第 1 章 §1 中定理 1), 我们容易得到群 SU(2) 的所有有限子群的描写 (可以在反方向作用). 任一不同于循环群这样的群 G^* 是 SO(3) 中某一个有限子群 G 的逆像. 于是产生了被称为二元群的下列群

$$D_n^8 = \Phi^{-1}(D_n), \quad \mathbf{T}^* = \Phi^{-1}(\mathbf{T}),$$
$$\mathbf{O}^* = \Phi^{-1}(\mathbf{O}), \quad \mathbf{I}^* = \Phi^{-1}(\mathbf{I}).$$

它们分别是二元二面体群, 二元四面体群, 二元八面体群和二元二十面体群. 二元群以及正交表示

$$\Phi: \mathrm{SU}(2) \to \mathrm{SO}(3)$$

整体上以自然的方式出现在描写自旋粒子的物理系统的状态中.

习 题

1. 在二十面体群 **I** 中, 除单位元子群外, 有 15 个共轭的 2 阶循环群, 10 个共轭的 3 阶循环子群和 6 个共轭的 5 阶循环子群. 证明: **I** 是一个单群.
2. 在群 **I** 与 A_5 之间建立一个同构.
3. 证明: 如果 H 是 SU(2) 或 SO(3) 中的一个奇阶有限子群, 则 H 是一个循环群.
4. 如果有限子群 $H \subset \mathrm{SU}(2)$ 不是任何子群 $G \subset \mathrm{SO}(3)$ 的逆像, 则 $|H| \equiv 1 \pmod 2$. 试证之.
5. 证明: 精确到共轭有

$$D_3^* = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}; \varepsilon^2 + \varepsilon + 1 = 0 \right\rangle.$$

6. 二元二十面体群 $\mathbf{I}^*$ 与群

$$\mathrm{SL}(2, Z_5) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| ad - bc = 1, a, b, c, d \in Z_5 \right\}$$

彼此之间有什么共同点?

7. 假设不同种类的 q 个原子 ($q < 200$) 以各种各样的方式位于 (不考虑任何化学联系) 正多面体 M 的顶点. 通过绕一个轴的旋转而得到的 "分子" 是不同的. 令 $f(M, q)$ 是不同分子的个数. 试推出公式

$$f(\triangle_4, q) = \frac{q^2}{12}(q^2 + 11),$$
$$f(\square_6, q) = \frac{q^2}{24}(q^6 + 17q^2 + 6),$$
$$f(\triangle_8, q) = \frac{q^2}{24}(q^4 + 3q^2 + 12q + 8).$$

8. 证明: 在四面体 $\triangle_4$ 中, 说明计算用 q 种颜色染多面体 M 的各面的不同色彩的个数的公式与习题 7 中公式一样, 而在立方体和八面体中公式互换位置.

§4 线性表示的特征标

1. 舒尔 (Schur) 引理和它的推论 在任一丰富的数学理论中往往有一些简单的 (但巧妙的) 想法成为该理论的基础. 下列论断是表示理论的奠基石之一.

定理 1 (舒尔引理) 假设 $(\Phi, V), (\Psi, W)$ 是群 G 的两个不可约复表示, $\sigma : V \to W$ 是一个线性映射, 满足

$$\Psi(g)\sigma = \sigma\Phi(g), \quad \forall g \in G. \tag{1}$$

那么

i) 如果表示 Φ 与 Ψ 不等价, 则 $\sigma = 0$;

ii) 如果 $V = W, \Phi = \Psi$, 则 $\sigma = \lambda\mathcal{E}$.

证明 如果 $\sigma = 0$, 则已成立. 所以可以认为 $\sigma \neq 0$, 且设 $V_0 = \operatorname{Ker}\sigma \subset V$.

因为对任意 $v_0 \in V_0, \sigma\Phi(g)v_0 = \Psi(g)\sigma v_0$, 所以 $\Phi(g)V_0 = V_0$, 即子空间 V_0 关于 G 是不变的. 由 (Φ, V) 的不可约性, 我们有 $V_0 = 0$ 或 $V_0 = V$. 等式 $V_0 = V$ 是不可能的, 这是因为 $\sigma \neq 0$. 因此 $\operatorname{Ker}\sigma = 0$.

类似地, 令 $W_1 = \operatorname{Im}\sigma \subset W$, 则有

$$w_1 \in W \Longrightarrow \Psi(g)w_1 = \Psi(g)\sigma(v_1) = \sigma(\Phi(g)v_1) = w_1' \in W_1,$$

于是 W_1 是 W 中的一个 G–不变子空间. 同样因为 $\sigma \neq 0 \Longrightarrow W_1 \neq 0$, 然而因为 (Ψ, W) 是一个不可约表示, 所以只能有 $W_1 = W$.

i) 因为 $\operatorname{Ker}\sigma = 0, \operatorname{Im}\sigma = W$, 所以 $\sigma : V \to W$ 是一个同构映射, 于是断言 i) 不是别的, 正是表示 Φ, Ψ 的等价的条件 (参见 § 1, 定义 2). 故断言 i) 证毕.

ii) 由条件 $\sigma : V \to V$ 是 V 上的线性算子. 设 λ 是它的一个特征值; 这个特征值总是存在的, 因为基域 $\mathbb{C}$ 是代数闭域. 线性算子 $\sigma_0 = \sigma - \lambda\mathcal{E}$ 有非平凡的核 (在核中包含特征向量) 且满足等式 $\Psi(g)\sigma_0 = \sigma_0\Phi(g)$. 按照前面证明的, 有 $\sigma_0 = 0$, 从而 $\sigma = \lambda\mathcal{E}$. □

推论 假设 $(\Phi, V), (\Psi, W)$ 是阶为 $|G|$ 的有限群 G 在域 $\mathbb{C}$ 上的两个不可约表示, $\sigma : V \to W$ 是任一线性映射. 那么平均映射

$$\widetilde{\sigma} = \frac{1}{|G|}\sum_{g \in G}\Psi(g)\sigma\Phi(g)^{-1}$$

有下列性质:

i) $\Phi \not\approx \Psi \Longrightarrow \widetilde{\sigma} = 0$;

ii) $V = W, \Phi = \Psi \Longrightarrow \widetilde{\sigma} = \lambda\mathcal{E}, \lambda = \dfrac{\operatorname{tr}\sigma}{\dim V}$.

证明 因为

$$\begin{aligned}\Psi(g)\tilde{\sigma}\Phi(g)^{-1} &= |G|^{-1}\sum_{h\in G}\Psi(g)\Psi(h)\sigma\Phi(h)^{-1}\Phi(g)^{-1}\\ &= |G|^{-1}\sum_{h}\Psi(gh)\sigma\Phi(gh)^{-1}\\ &= |G|^{-1}\sum_{t\in G}\Psi(t)\sigma\Phi(t)^{-1} = \tilde{\sigma},\end{aligned}$$

所以 $\Psi(g)\widetilde{\sigma} = \widetilde{\sigma}\Phi(g), \forall g \in G$. 由 Schur 引理立即得到两个断言, 同时有关常数 λ 的更详细的说明, 可由下列关系推出:

$$\begin{aligned}(\dim V)\lambda = \operatorname{tr}\lambda\mathcal{E} = \operatorname{tr}\widetilde{\sigma} &= |G|^{-1}\sum_{g\in G}\operatorname{tr}\Phi(g)\sigma\Phi(g)^{-1}\\ &= |G|^{-1}\sum_{g\in G}\operatorname{tr}\sigma = \operatorname{tr}\sigma.\end{aligned}$$

这里我们引用了迹函数的熟悉的性质: $\operatorname{tr}CAC^{-1} = \operatorname{tr}A$. □

我们需要推论的矩阵形式. 为此, 我们在两个空间 V, W 中选择基分别为:

$$V = \langle e_i | i \in I\rangle, \quad W = \langle f_j | j \in J\rangle.$$

在这两组基下, 将我们的映射用矩阵表示:

$$\begin{aligned}&\Phi_g = (\varphi_{ii'}(g)), \quad \Psi_g = (\psi_{jj'}(g)),\\ &\sigma = (\sigma_{ji}), \quad \widetilde{\sigma} = (\widetilde{\sigma}_{ji}); \quad i, i' \in I, \quad j, j' \in J.\end{aligned}$$

由 $\widetilde{\sigma}$ 的定义

$$\widetilde{\sigma}_{ji} = |G|^{-1}\sum_{g\in G, i'\in I, j'\in J}\psi_{jj'}(g)\sigma_{j'i'}\varphi_{i'i}(g^{-1}). \tag{2}$$

因为我们的映射 $\sigma : V \to W$ 是完全任意选取的, 所以我们可以让

$$\sigma_{ji} = 0 \quad \forall (j, i) \neq (j_0, i_0); \quad \sigma_{j_0 i_0} = 1. \tag{3}$$

那么由断言 i) 推得下列关系

$$|G|^{-1}\sum_{g\in G}\psi_{jj_0}(g)\cdot\varphi_{i_0 i}(g^{-1}) = 0, \quad \forall i, i_0, j, j_0 \tag{4}$$

(这里 Φ 和 Ψ 是不等价的表示).

如果现在令 $V = W$ 且 $\Phi = \Psi$, 那么

$$\begin{aligned}&\operatorname{tr}\sigma = \sum_{i}\sigma_{ii} = \sum_{i', j'}\delta_{j'i'}\sigma_{j'i'},\\ &\widetilde{\sigma} = \frac{\operatorname{tr}\sigma}{\dim V}\mathcal{E} \Longrightarrow \widetilde{\sigma}_{ji} = \delta_{ji}\frac{\operatorname{tr}\sigma}{\dim V} = \frac{\delta_{ji}}{\dim V}\sum_{i', j'}\delta_{j', i'}\sigma_{j'i'}.\end{aligned}$$

对照所得到的等式 (2), 我们有

$$|G|^{-1}\sum_{g\in G,i',j'}\varphi_{jj'}(g)\sigma_{j'i'}\varphi_{i'i}(g^{-1})=\frac{1}{\dim V}\sum_{i',j'}\delta_{ji}\delta_{j'i'}\sigma_{j'i'},$$

由此并由 σ 选择的任意性 (见 (3)) 得到结论: 推论的断言 ii) 适合关系

$$|G|^{-1}\sum_{g\in G}\varphi_{jj_0}(g)\varphi_{i_0 i}(g^{-1})=\begin{cases}\dfrac{\delta_{ji}}{\dim V}, & \text{如果 } j_0=i_0,\\ 0, & \text{如果 } j_0\neq i_0.\end{cases}\tag{5}$$

关系 (4) 和 (5) 包含了我们所需要的信息. □

2. 表示的特征标 设 (Φ,V) 是群 G 的一个复有限维线性表示, 定义一个 G 到 $\mathbb{C}$ 的函数

$$\chi_\Phi : G\to\mathbb{C}$$
$$\chi_\Phi(g)=\mathrm{tr}\Phi(g),\quad g\in G,$$

则称 χ_Φ **为表示 Φ 的特征标**, 记为 χ_V 或 χ (当不引起混淆时).

设 $\Phi_g=(\varphi_{ij}(g))$ 是算子 $\Phi(g)$ 在空间 V 的某一个基下的矩阵, 而 $\lambda_1,\cdots,\lambda_n(n=\dim V)$ 是该矩阵的特征根 (可以有重根). 由定义

$$\chi_\Phi(g)=\chi_V(g)=\sum_{i=1}^n\varphi_{ii}(g)=\sum_{i=1}^n\lambda_i.$$

如果 C 是任一可逆矩阵, 那么

$$\mathrm{tr}C\Phi_gC^{-1}=\mathrm{tr}\Phi_g.$$

但是我们知道, 对于任意等价于 Φ 的表示 Ψ 有形式 $g\mapsto C\Phi_gC^{-1}$. 因此同构的 (等价的) 表示的特征标相同. 这表明, 特征标的概念定义是合理的.

我们也指出一系列特征标的等价性质.

命题 假设 χ_Φ 是群 G 的复线性表示 (Φ,V) 的特征标. 则

i) $\chi_\Phi(e)=\dim V$;

ii) $\chi_\Phi(hgh^{-1})=\chi_\Phi(g),\forall g,h\in G$, 也就是说, χ_Φ 是在 G 的共轭元素类上不变的函数;

iii) $\chi_\Phi(g^{-1})=\overline{\chi_\Phi(g)}$, 对于 G 的任意有限阶元 g (这里的横线表示复共轭);

iv) 对于表示的直和 $\Phi=\Phi'\dotplus\Phi''$, 相应地有特征标的和 $\chi_\Phi=\chi_{\Phi'}+\chi_{\Phi''}$.

证明 事实上, $\chi_\Phi(e)=\mathrm{tr}\Phi(e)=\mathrm{tr}\mathcal{E}=\dim V$. 又

$$\chi_\Phi(hgh^{-1})=\mathrm{tr}\Phi(hgh^{-1})=\mathrm{tr}\Phi(h)\Phi(g)\Phi(h)^{-1}=\mathrm{tr}\Phi(g)=\chi_\Phi(g).$$

对于 iii) 的证明, 我们注意到

$$g^m = e \Longrightarrow \Phi(g)^m = \mathcal{E},$$

且如果 $\lambda_1, \cdots, \lambda_n$ 是算子 $\Phi(g)$ 的特征根, 则 $\lambda_1^k, \cdots, \lambda_n^k$ 就是算子 $\Phi(g)^k$ 的特征根. 特别地, $\lambda_i^m = 1, 1 \leqslant i \leqslant n$, 于是 $|\lambda_i| = 1, \overline{\lambda_i} = \lambda_i^{-1}$. 因此

$$\chi_\Phi(g^{-1}) = \mathrm{tr}\Phi(g^{-1}) = \sum_i \lambda_i^{-1} = \sum_i \overline{\lambda}_i = \overline{\sum_i \lambda_i} = \overline{\chi_\Phi(g)}.$$

最后, 如果 $\Phi = \Phi' \dot{+} \Phi''$, 那么我们知道, 适当选取表示空间 V 的一个基, 所有矩阵 $\Phi_g, g \in G$, 有形式

$$\Phi_g = \begin{pmatrix} \Phi'_g & 0 \\ 0 & \Phi''_g \end{pmatrix},$$

于是 $\mathrm{tr}\Phi_g = \mathrm{tr}\Phi'_g + \mathrm{tr}\Phi''_g$. 这表明 $\chi_\Phi(g) = \chi_{\Phi'}(g) + \chi_{\Phi''}(g)$. □

我们指出, 当 $n = \dim V = 1$ 时, 有 $\chi_\Phi(g) = \Phi(g)$, 但当 $n > 1$ 时, 特征标 χ_Φ 不是 G 到 C^* 的同态.

例 1 我们来看群 SU(2) 和它的自然 2 维表示. 令 χ 是它的特征标. 按照第 1 章 §1 中 (5), 任意矩阵 $g \in \mathrm{SU}(2)$ 共轭于矩阵

$$b_\varphi = \begin{pmatrix} e^{i\varphi/2} & 0 \\ 0 & e^{-i\varphi/2} \end{pmatrix}, \quad 0 \leqslant \varphi < 2\pi,$$

于是群 SU(2) 的共轭元素类被所指区间中实数 φ 参数化. 根据特征标的性质 ii), 我们有

$$\chi(g) = \chi(hb_\varphi h^{-1}) = \chi(b_\varphi) = e^{i\varphi/2} + e^{-i\varphi/2} = 2\cos\varphi/2.$$

在标准表示 $\Phi : \mathrm{SU}(2) \to \mathrm{SO}(3)$ 下, 矩阵 b_φ 变为矩阵

$$B_\varphi = \begin{pmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

该矩阵同样可作为正交矩阵群 SO(3) 的共轭类的适当的代表. 显然,

$$\chi_\Phi(B_\varphi) = 1 + 2\cos\varphi. \tag{6}$$

公式 (6) 我们在下面将用到.

由 G 到 $\mathbb{C}$ 的所有函数的集合 $\mathbb{C}^G = \{G \to \mathbb{C}\}$ 具有 $\mathbb{C}$ 上向量空间的自然的结构: 对于 $\alpha_1, \alpha_2 \in \mathbb{C}, \chi_1, \chi_2 \in \mathbb{C}^G$, 让 $\alpha_1\chi_1 + \alpha_2\chi_2$ 表示为这样的函数:

$$(\alpha_1\chi_1 + \alpha_2\chi_2)(g) = \alpha_1\chi(g) + \alpha_2\chi(g).$$

$\mathbb{C}^G$ 中的一个函数称为**中心的**, 如果它在群 G 的共轭类上是固定不变的. 所有中心函数显然构成 $\mathbb{C}^G$ 中的一个向量子空间, 我们将它表示为 $X_{\mathbb{C}}(G)$. 一般地说, $X_{\mathbb{C}}(G)$ 是一个无限维空间, 但是如果群 G 中只有有限个共轭元素类 $\mathcal{K}_1, \mathcal{K}_2, \cdots, \mathcal{K}_r$ (对于有限群这总是对的), 则 $X_{\mathbb{C}}(G)$ 是有限维空间. 例如

$$X_{\mathbb{C}}(G) = \langle \Gamma_1, \Gamma_2, \cdots, \Gamma_r \rangle_{\mathbb{C}},$$

这里

$$\Gamma_i(g) = \begin{cases} 1, & \text{如果 } g \in \mathcal{K}_i, \\ 0, & \text{如果 } g \notin \mathcal{K}_i. \end{cases} \tag{7}$$

根据命题 ii) 的证明, 群 G 的特征标属于空间 $X_{\mathbb{C}}(G)$. 我们看到, 它们上的一个非自然子空间实际上等于 $X_{\mathbb{C}}(G)$, 至少对于有限群 G 是如此.

下面我们假设群 G 是有限的. 将 $\mathbb{C}^G$ 变为具有内积

$$(\sigma, \tau)_G = \frac{1}{|G|} \sum_{g \in G} \sigma(g)\overline{\tau(g)}, \quad \sigma, \tau \in \mathbb{C}^G, \tag{8}$$

的埃尔米特空间. 容易验证, 型 $(\sigma, \tau) \mapsto (\sigma, \tau)_G$ 满足非退化埃尔米特型的所有性质. 它在子空间 $X_{\mathbb{C}}(G) \subset \mathbb{C}^G$ 上的缩小是非常有益的工具, 尤其是对于研究线性表示的特征标.

定理 2　假设 Φ, Ψ 是有限群 G 的不可约复表示. 那么

$$(\chi_\Phi, \chi_\Psi)_G = \begin{cases} 1, & \text{如果 } \Phi \approx \Psi, \\ 0, & \text{如果 } \Phi \not\approx \Psi. \end{cases} \tag{9}$$

证明　在矩阵记法里有

$$\chi_\Phi(g) = \sum_{i=1}^{n} \varphi_{ii}(g), \quad \chi_\Psi(g) = \sum_{i=1}^{n} \psi_{ii}(g).$$

在关系 (4) 中让 $i_0 = i, j_0 = j$, 然后就 i 和 j 求和 (在 i, j 允许范围内), 对于群 G 的任意不可约的等价表示 Φ, Ψ 我们得到

$$\begin{aligned} 0 &= |G|^{-1} \sum_{g,i,j} \psi_{jj}(g)\varphi_{ii}(g) = |G|^{-1} \sum_{g} \left(\sum_{j} \psi_{jj}(g) \right) \left(\sum_{i} \varphi_{ii}(g^{-1}) \right) \\ &= |G|^{-1} \sum_{g \in G} \chi_\Psi(g)\chi_\Phi(g^{-1}) = |G|^{-1} \sum_{g \in G} \chi_\Psi(g)\overline{\chi_\Phi(g)} \\ &= (\chi_\Psi, \chi_\Phi)_G. \end{aligned}$$

现在我们应用关系式 (5) (当 $i_0 = i, j_0 = j$):

$$1 = \frac{\sum_{j,i} \delta_{ji}}{\dim V} = \frac{1}{|G|} \sum_{g \in G} \left(\sum_j \varphi_{jj}(g) \right) \left(\sum_i \varphi_{ii}(g^{-1}) \right)$$
$$= |G|^{-1} \sum_{g \in G} \chi_\Phi(g) \chi_\Phi(g^{-1}) = (\chi_\Phi, \chi_\Phi)_G.$$

因为同构的表示的特征标相同, 所以当 $\Phi \approx \Psi$ 时 $(\chi_\Phi, \chi_\Psi)_G = 1$. □

关系 (9) 称为**特征标的 (第一) 正交关系**.

推论 假设

$$V = V_1 \oplus \cdots \oplus V_k \tag{10}$$

是复 G–空间 V 的不可约 G–子空间 V_i 的直和分解. 如果 W 是具有特征标 χ_W 的某一个不可约 G–子空间, 那么同构于 W 的 (10) 中直和项 V_i 的个数等于 $(\chi_V, \chi_W)_G$ 且不取决于分解的方法 (W 在 G–空间 V 中出现的重数). 具有同样特征标的两个表示 (两个 G–空间) 是同构的.

证明 正如我们前面 (命题 iv) 已经看到的,

$$\chi_V = \chi_{V_1} + \cdots + \chi_{V_k}, \quad \text{因此} \quad (\chi_V, \chi_W)_G = (\chi_{V_1}, \chi_W)_G + \cdots + (\chi_{V_k}, \chi_W)_G.$$

根据定理 2, 右边应该是 k 个 0 和 1 的和, 而且 1 的个数等于同构于 W 的 G–子空间 V_i 的个数, 但是内积 $(\chi_V, \chi_W)_G$ 一般不依赖于分解的分解方式 (参见定义关系 (8)), 于是我们同时证明了 W 出现在 G–空间 V 中重数的不变性.

对于两个具有相同特征标 $\chi = \chi_V = \chi_{V'}$ 的 G–空间 V, V', 包含在它们分解式中的同构于某一给定不可约 G–空间 W 的直和项的重数相等, 它们就等于 $(\chi, \chi_W)_G$. 因此在两个不可约直和分解式

$$V = \bigoplus_{i=1}^{k} V_i, \quad V' = \bigoplus_{j=1}^{l} V'_j$$

中, 我们可以认为 $k = l$, 且 $V'_i \cong V_i, 1 \leqslant i \leqslant k$. 从而 G–空间 V 和 V' 本身也同构. □

Maschke 定理的证明后所做的说明和定理 2 的推论给出了有限群 G 的任一复线性表示 (Φ, V) 的特征标 χ_Φ 表示为整数线性组合形式的可能性:

$$\chi_\Phi = \sum_{i=1}^{s} m_i \chi_i.$$

其中 m_i 是 (Φ, V) 的分解式中某一不可约表示 (Φ_i, V_i) 的重数, 且当 $i \neq j$ 时, $\Phi_i \not\approx \Phi_j$. 应用正交关系 (9), 我们可以写

$$(\chi_\Phi, \chi_\Phi)_G = \sum_{i=1}^{s} m_i^2. \tag{11}$$

于是, 任意复表示 Φ 的特征标 χ_Φ 的内积 $(\chi_\Phi, \chi_\Phi)_G$ 总是一个整数. 它等于 1 当且仅当 Φ 本身是一个不可约表示. □

我们得到了出色的结果. 特征标或 "表示的迹", 对于每个单个的线性算子 $\Phi(g)$ 有很少的信息, 但对于它们的全部 $\{\Phi(g)|g \in G\}$, 也就是表示 Φ 本身, 却表现出了极重要的性质.

例 2 我们来证明群 A_4, S_4, A_5 通过三维空间旋转的表示在 $\mathbb{C}$ 上的不可约性. 为此需要回到 §3 中定理 2 的推论上来并应用公式 (6) 和 (11). §3 中描写的表示 Φ 表明, 如果 π 是一个 q 阶置换, 那么 $\Phi(\pi)$ 是围绕某一轴的 $k \cdot 2\pi/q$ 角度的旋转, 这里 $\mathrm{g.c.d}(k, q) = 1$. 因此, 由公式 (6), 特征标 $\chi = \chi_\Phi$ 的值可以直接算出:

$$\chi(\pi) = 1 + 2\cos k\frac{2\pi}{q} = 3, -1, 0, 1, \frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2},$$

对于相应的 $q = 1, 2, 3, 4, 5(k = \pm 1), 5(k = \pm 2)$. 我们指出

$$\frac{1+\sqrt{5}}{2} = \mathrm{tr}\begin{pmatrix} \varepsilon & 0 & 0 \\ 0 & \varepsilon^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix} = \varepsilon + \varepsilon^{-1} + 1,$$

$$\frac{1-\sqrt{5}}{2} = \varepsilon^2 + \varepsilon^{-2} + 1, \quad \varepsilon = \exp\left(\frac{2\pi i}{5}\right).$$

在 [BA I] 第 4 章 §2 习题 13 表明, 一个置换 π 可分解为不相交循环置换的乘积, 由此我们可以计算置换 π 的阶. 按照共轭类的元素的分布以前曾得到表的形式, 现在添加上特征标 χ 的值, 有下表:

12	1	3	4	4
A_4	e	(1 2)(3 4)	(1 2 3)	(1 3 2)
χ	3	−1	0	0

24	1	3	6	8	6
S_4	e	(1 2)(3 4)	(1 2)	(1 2 3)	(1 2 3 4)
χ	3	−1	−1	0	1

60	1	15	20	12	12
A_5	e	(1 2)(3 4)	(1 2 3)	(1 2 3 4 5)	(1 2 3 5 4)
χ	3	−1	0	$(1+\sqrt{5})/2$	$(1-\sqrt{5})/2$

.

下列关系

$$(\chi,\chi)_{A_4}=\frac{1}{12}\{1\cdot 3^2+3(-1)^2+4\cdot 0^2+4\cdot 0^2\}=1,$$
$$(\chi,\chi)_{S_4}=\frac{1}{24}\{1\cdot 3^2+3(-1)^2+6\cdot(-1)^2+8\cdot 0^2+6\cdot 1^2\}=1,$$
$$(\chi,\chi)_{A_5}=\frac{1}{60}\left\{1\cdot 3^2+15\cdot(-1)^2+20\cdot 0^2+12\left(\frac{1+\sqrt{5}}{2}\right)^2+12\left(\frac{1-\sqrt{5}}{2}\right)^2\right\}=1$$

表明, 具有特征标 χ 的表示 Φ 在 $\mathbb{C}$ 上不可约 (参见 (11)).

习 题

1. 设 Φ,Ψ 是有限群 G 的不可约复表示. 试得出定理 2 的推广

$$|G|^{-1}\sum_g \chi_\Psi(hg)\overline{\chi_\Phi(g)}=\delta_{\Phi,\Psi}\frac{\chi_\Phi(h)}{\chi_\Phi(e)}.$$

这里 h 是 G 的任意元, $\delta_{\Phi,\Psi}=1$ 或 $\delta_{\Phi,\Psi}=0$ 取决于 Φ 与 Ψ 的等价或不等价.

2. 将建立在特征标上的不可约判别准则应用到 §2 第 1 目例 1 中的群 S_3 的表示 $\Phi^{(3)}$.

3. 利用舒尔引理证明: 交换群 G 的 $\mathbb{C}$ 上的所有不可约表示都是一维的.

4. 如果群 G 有一个自同构 τ, 那么这个群的每个线性表示 (Φ,V) 也伴随着一个表示 (Φ^τ,V), 其中 Φ^τ 规定为 $\Phi^\tau(g)=\Phi(\tau(g))$. 验证这一结论, 并证明, 如果 Φ 不可约, 那么 Φ^τ 也不可约. 通常, $\Phi^\tau\approx\Phi$, 但是常常有得到新的表示的情况. 如果 τ 是内自同构, 情形如何呢?

令 $G=A_5,\Phi$ 是例 2 中所见的表示. 映射 $\tau:\pi\mapsto(1\ 2)\pi(1\ 2)^{-1}$ 是 A_5 的一个 (内) 自同构, 它置换代表元 $(1\ 2\ 3\ 4\ 5)$ 和代表元 $(1\ 2\ 3\ 5\ 4)$ 所在的两个共轭类. 其相应的特征标 χ 和 χ^τ 的值也分别对调了 $(1+\sqrt{5})/2$ 和 $(1-\sqrt{5})/2$ 的位置. 证明: 这两个特征标 χ^τ 与 χ 不等价.

5. 设 $\Phi:G\to\mathrm{U}(n),\Psi:G\to\mathrm{U}(n)$ 为有限群 G 的两个等价的不可约酉表示. 证明: 存在酉矩阵 C 使

$$C\Phi_gC^{-1}=\Psi_g,\quad \forall g\in G.$$

6. 证明拥有 $\mathbb{C}$ 上忠实不可约表示的有限群 G 的中心 $Z(G)$ 总是平凡的或循环的.

7. 设 $g\mapsto\Phi_g,g\mapsto\Psi_g$ 为有限群 G 的两个矩阵复表示. 假设对于每个 $g\in G$, 存在非退化矩阵 C_g 使 $C_g\Phi_gC_g^{-1}=\Psi_g$. 证明, 存在不依赖于 g 的非退化矩阵 C, 使 $C\Phi_gC^{-1}=\Psi_g$.

§5 有限群的不可约表示

1. 不可约表示的个数 在有限群的情况下, 前面的研究允许我们来回答群表示理论的一些基本问题. 其中之一是下面的

定理 1　$\mathbb{C}$ 上的有限群 G 的两两不等价的不可约表示的个数等于群 G 的共轭元素类的个数.

如果我们注意到群 G 的共轭元素类的个数 r 被我们解释为 G 上中心复值函数空间 $X_{\mathbb{C}}(G)$ 的维数 (见 §4 (7)), 定理的证明包含在引理 1 和引理 2 中. 因为线性表示的特征标是中心函数, 所以它们在 $X_{\mathbb{C}}(G)$ 中生成一个维数 $s \leqslant r$ 的线性子空间. 由 §4 定理 2, 不可约表示的特征标是这个子空间的一个标准正交基. 于是, 我们关心的数等于 s, 且它不超于 r. 剩下只要证明 $s = r$.

引理 1　假设 Γ 是有限群 G 上的一个中心函数, (Φ, V) 是 $\mathbb{C}$ 上具有特征标 χ_Φ 的一个不可约表示.

那么对于线性算子

$$\Phi_\Gamma = \sum_{h\in G} \overline{\Gamma}(h)\Phi(h) : V \to V$$

有 $\Phi_\Gamma = \lambda\mathcal{E}$, 其中

$$\lambda = \frac{|G|}{\chi_\Phi(e)}(\chi_\Phi, \Gamma)_G$$

($\overline{\Gamma}$ 是由等式 $\overline{\Gamma}(g) = \overline{\Gamma(g)}$ 所确定的一个中心函数).

证明　因为 Γ 是一个中心函数, 所以

$$\begin{aligned}\Phi(g)\Phi_\Gamma\Phi(g)^{-1} &= \sum_{h\in G} \overline{\Gamma}(h)\Phi(g)\Phi(h)\Phi(g^{-1}) \\ &= \sum_{h\in G} \overline{\Gamma(ghg^{-1})}\Phi(ghg^{-1}) \\ &= \sum_{h\in G} \overline{\Gamma}(t)\Phi(t) = \Phi_\Gamma.\end{aligned}$$

因此, $\Phi_\Gamma\Phi(g) = \Phi(g)\Phi_\Gamma, \forall g \in G$. 舒尔引理 (§4 定理 1) 运用到情况 $\sigma = \Phi_\Gamma$, 表明 $\Phi_\Gamma = \lambda\mathcal{E}$. 算出这个等式两边的算子的迹, 我们有

$$\begin{aligned}\lambda\chi_\Phi(e) &= \lambda \dim V = \operatorname{tr}\lambda\mathcal{E} = \operatorname{tr}\Phi_\Gamma \\ &= \sum_{h\in G} \overline{\Gamma}(h)\operatorname{tr}\Phi(h) \\ &= |G|\left\{|G|^{-1}\sum_{h\in G}\chi_\Phi(h)\overline{\Gamma(h)}\right\} \\ &= |G|\left(\chi_\Phi, \Gamma\right)_G.\end{aligned}$$

□

引理 2　$\mathbb{C}$ 上群 G 的所有两两不等价的不可约表示的特征标 $\chi_1, \chi_2, \cdots, \chi_s$ 构成空间 $X_{\mathbb{C}}(G)$ 的一个标准正交基.

证明 由 §4 定理 2, $\chi_1, \cdots, \chi_s$ 是正交的, 且它们可以含于空间 $X_{\mathbb{C}}(G)$ 的标准正交基. 令 Γ 是任一与所有 χ_i 正交的 (即 $(\chi_i, \Gamma) = 0$) 的中心函数. 那么由引理 1, 对应于具有特征标 χ_i 的表示 $\Phi^{(i)}$ 的线性算子 $\Phi_\Gamma^{(i)}$ 等于零.

由 Maschke 定理, 任一复表示 Φ 可以分解为直和

$$\Phi = m_1\Phi^{(1)} \dotplus \cdots \dotplus m_s\Phi^{(s)},$$

对于某些重数 $m_1, \cdots, m_s$. 对应于由关系式

$$\Phi_\Gamma = \sum_{h \in G} \overline{\Gamma}(h)\Phi(h)$$

定义的算子 Φ_Γ 的这一分解, 我们有

$$\Phi_\Gamma = m_1\Phi_\Gamma^{(1)} \dotplus \cdots \dotplus m_s\Phi_\Gamma^{(s)} = 0.$$

特别地, 这与线性算子 ρ_Γ 有关, 这里 ρ 是一个正则表示 (参见 §1 例 5). 但在这种情况下, 我们有 (为了避免写 e_e, 这里暂时用符号 1 来表示群 G 的单位元)

$$\begin{aligned} 0 = \rho_\Gamma(e_1) &= \sum_{h \in G} \overline{\Gamma}(h)\rho(h)e_1 \\ &= \sum_{h \in G} \overline{\Gamma}(h)e_h \Longrightarrow \overline{\Gamma}(h) = 0. \end{aligned}$$

因为这个等式对任何 $h \in G$ 成立, 所以 $\overline{\Gamma} = 0$, 从而 $\Gamma = 0$. □

例 1 将定理 1 运用到对称群 S_3, 我们知道, 这个群恰好有三个不可约复表示. 不需要寻找它们: 在 §2 第 1 目最后包含了所有必要的信息. 顺便说一下, 表示 $\Phi^{(1)}, \Phi^{(2)}, \Phi^{(3)}$ 的维数的平方满足关系 $1^2 + 1^2 + 2^2 = 6 = |S_3|$. 下面我们将看到, 在一般情况下也有类似的关系.

2. 不可约表示的维数 我们来考察一些更详细的正则表示 $(\rho, \langle e_g | g \in G\rangle_{\mathbb{C}})$. 我们用 R_h 来表示线性算子 $\rho(h)$ 在给定基 $\{e_g | g \in G\}$ 下的矩阵. 因为 $\rho(h)e_g = e_{hg}$, 所以当 $h \neq e$ 时, 矩阵 R_h 的所有对角线元素都等于零, 从而 $\mathrm{tr} R_h = 0$. 于是

$$\chi_\rho(e) = |G|, \ \chi_\rho(h) = 0, \quad \forall h \neq e. \tag{1}$$

现在令 (Φ, V) 是 $\mathbb{C}$ 上群 G 的任意不可约表示. 作为 §4 定理 2 的推论所证明的, Φ 在 ρ 中出现的重数等于内积 $(\chi_\rho, \chi_\Phi)_G$. 由 (1)

$$\begin{aligned} (\chi_\rho, \chi_\Phi)_G &= |G|^{-1} \sum_{h \in G} \chi_\rho(h)\overline{\chi_\Phi(h)} \\ &= |G|^{-1}\chi_\rho(e)\overline{\chi_\Phi(e)} = |G|^{-1}|G|\chi_\Phi(e) = \dim V. \end{aligned} \tag{2}$$

我们看到, 每个不可约表示 (精确到等价) 在正则表示中出现, 其出现的重数等于它的维数. 按照定理 1, 有 r 个两两不等价的不可约表示

$$\Phi^{(1)}, \Phi^{(2)}, \cdots, \Phi^{(r)},$$

(这里 r 为群 G 的共轭元素类的个数), 它们相应的特征标

$$\chi_1, \chi_2, \cdots, \chi_r, \quad \chi_i = \chi_\Phi^{(i)},$$

维数分别为

$$n_1, n_2, \cdots, n_r, \quad n_i = \chi_i(e).$$

通常取满足 $\chi_1(g) = 1, \forall g \in G$, 的单位表示作为 $\Phi^{(1)}$. 关系式 (2) 表明

$$\rho = n_1\Phi^{(1)} \dot{+} \cdots \dot{+} n_r\Phi^{(r)},$$

由此得到

$$\chi_\rho = n_1\chi_1 + \cdots + n_r\chi_r.$$

特别地,

$$\begin{aligned} |G| = \chi_\rho(e) &= n_1\chi_1(e) + \cdots + n_r\chi_r(e) \\ &= n_1^2 + \cdots + n_r^2. \end{aligned}$$

定理 2 每个不可约表示 $\Phi^{(i)}$ 出现在正则表示 ρ 的分解中, 其出现的重数等于自身的维数. 有限群 G 的阶 $|G|$ 和它的所有不可约表示的维数 $n_1, \cdots, n_r$ 满足如下关系:

$$\sum_{i=1}^{r} n_i^2 = |G|. \tag{3}$$

对于阶数不大的群, 这个漂亮的关系式 (3) 对于找出所有的维数 $n_1, \cdots, n_r$ 已经足够了, 不过在一般情况下, 当然还需要一些补充的考虑.

关于不可约表示的特征标 (或简称为不可约特征标) 的信息写成下列表是方便的

G	e	g_2	g_3	$\cdots$	g_r
χ_1	n_1	$\chi_1(g_2)$	$\chi_1(g_3)$	$\cdots$	$\chi_1(g_r)$
χ_2	n_2	$\chi_2(g_2)$	$\chi_2(g_3)$	$\cdots$	$\chi_2(g_r)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
χ_r	n_r	$\chi_r(g_2)$	$\chi_r(g_3)$	$\cdots$	$\chi_r(g_r)$

,

该表称为特征标表. 第一行是群 G 的 r 个共轭类 $\mathcal{K}_i = g_i^G$ 的代表. 例如, 群 S_3 的特征标表为

S_3	e	$(1\ 2)$	$(1\ 2\ 3)$
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

(对照 §2 第 1 目后面的表). 与通常一样, 我们用 $C(g) = C_G(g)$ 表示元素 $g \in G$ 在群 G 中的中心化子. 我们知道, $|C(g)||g^G| = |G|$ (见第 1 章 §3 第 2 目). 于是, §4 的关系 (9) (第一正交关系) 可以改写为

$$
\begin{aligned}
\sum_{j=1}^{r} \frac{\chi_i(g_j)}{\sqrt{|C(g_j)|}} \overline{\frac{\chi_k(g_j)}{\sqrt{|C(g_j)|}}} &= \frac{1}{|G|} \sum_{j=1}^{r} \frac{|G|}{|C(g_j)|} \chi_i(g_j)\overline{\chi_k(g_j)} \\
&= \frac{1}{|G|} \sum_{j=1}^{r} |g_i^G| \chi_i(g_j)\overline{x_k(g_j)} \\
&= \frac{1}{|G|} \sum_{g \in G} \chi_i(g)\overline{\chi_k(g)} \\
&= (\chi_i, \chi_k)_G = \delta_{ik},
\end{aligned}
$$

这表明, $r \times r$ 矩阵

$$
M = \left(\frac{\chi_i(g_j)}{\sqrt{|C(g_j)|}} \right)
$$

按行是酉矩阵. 但按行酉性等同于按列的酉性 $(M \cdot {}^t\overline{M} = E = {}^t\overline{M} \cdot M)$, 于是

$$
\sum_i \frac{\chi_i(g_j)}{\sqrt{|C(g_j)|}} \overline{\frac{\chi_i(g_k)}{\sqrt{|C(g_k)|}}} = \delta_{jk},
$$

或更详细地写为

$$
\sum_{i=1}^{r} \chi_i(g)\overline{\chi_i(h)} = \begin{cases} 0, & \text{如果 } g \text{ 和 } h \text{不共轭}, \\ |C_G(g)|, & \text{如果 } g \text{ 和 } h \text{共轭}. \end{cases} \tag{4}
$$

关系式 (4) 称为特征标的第二正交关系.

3. 交换群的表示 §1 例 6 中循环群的表示的描写容许我们作下列自然的推广.

定理 3 $\mathbb{C}$ 上有限交换群 A 的每个不可约表示的维数为 1. 这种两两不等价的表示的个数等于 A 的阶 $|A|$. 反之, 如果群 A 的每个不可约表示的维数为 1, 那么 A 是交换群.

证明　因为交换群 A 的共轭类的个数等于它的阶, 所以前两个结论可由定理 2 推得 (也可参见 §4 习题 3). 现在假设关系式 (3) 中所有 n_i 等于 1, 则我们有 $r=|A|$, 这等于说群是交换的. □

定义　假设 A 是一个交换群. 群 A 到复数域乘法群 $\mathbb{C}^*$ 的同态集合

$$\hat{A}=\mathrm{Hom}(A,\mathbb{C}^*)$$

与算子逐项乘法

$$(\chi_1\chi_2)(a)=\chi_1(a)\chi_2(a)$$

$(\chi_i\in\hat{A},a\in A)$ 一起, 称为 $\mathbb{C}$ 上群 A 的**特征标群**$(\chi^{-1}=\overline{\chi})$.

定理 4　群 A 与群 $\hat{A}$ 同构.

证明　由定理 3, 我们知道在任何情况下有 $|A|=|\hat{A}|$. 根据第 2 章 §3 的结果, 群 A 分解为循环群 $A_i=\langle a_i\rangle$ 的直积

$$A=A_1\times A_2\times\cdots\times A_k$$

(它们是不是准素循环群并不重要; 我们采用的乘法记号为 A 中乘法). 如果 $|A_i|=s_i$ 且 ε_i 为 1 的 s_i 次本原根, 那么对于 A 中每个元 $a=a_1^{t_1}a_2^{t_2}\cdots a_k^{t_k}$, 其特征标 $\chi_a\in\hat{A}$ 由关系式

$$\chi_a\left(a_1^{r_1}a_2^{r_2}\cdots a_k^{r_k}\right)=\varepsilon_1^{r_1t_1}\varepsilon_2^{r_2t_2}\cdots\varepsilon_k^{r_kt_k}$$

所确定. 显然, $\chi_a\chi_{a'}=\chi_{aa'}$ (见定义). 如果

$$a=a_1^{t_1}a_2^{t_2}\cdots a_k^{t_k}\neq a_1^{t_1'}a_2^{t_2'}\cdots a_k^{t_k'}=a',$$

那么存在指数 i 使 $t_i\neq t_i'$. 于是

$$\chi_a(a_i)=\varepsilon_i^{t_i}\neq\varepsilon_i^{t_i'}=\chi_{a'}(a_i).$$

从而所有特征标 χ_a 两两不同, 且映射 $a\mapsto\chi_a$ 建立了 A 与 $\hat{A}$ 的一个所要求的同构. □

定理 4 的证明方法显然给出了交换群的所有不可约表示的明显的结构.

例　假设 V_{2^n} 是一个阶为 2^n 的初等交换群, χ 是它的一个不可约复特征标且 χ 不同于单位表示, 即 $\chi(a)\neq 1$, 对于某 $a\in V_{2^n}$. 那么 $\mathrm{Ker}\chi=B\cong V_{2^{n-1}}$ 且有分解式 $V_{2^n}=B\cup aB$ 为 B 的陪集分解, 所以

$$\chi(a^ib)=(-1)^i,\quad i=0,1.$$

特别地, 克莱因四元群 V_4 (关于它的表示在第 1 章 §2 问题 2 中谈到了) 有下列特征标表:

V_4	e	a	b	ab
χ_1	1	1	1	1
χ_2	1	-1	1	-1
χ_3	1	1	-1	-1
χ_4	1	-1	-1	1

交换群的表示的结果也容许我们去得到有关任意有限群的表示的一些信息.

定理 5 $\mathbb{C}$ 上有限群 G 的一维表示与商群 G/G' (这里 G' 为群 G 的换位子群) 的不可约表示之间存在一一对应. 它们的个数等于指数 $(G:G')$.

证明 我们首先进行一般的讨论. 设 G 是任一个群, K 是它的一个正规子群. 如果 Φ 是群 G 的一个表示, 其核 $\mathrm{Ker}\Phi \supset K$, 那么我们可以确定商群 G/K 的一个表示 $\overline{\Phi}$:

$$\overline{\Phi}(gK) = \Phi(g), g \in G.$$

这个定义的合理性是显然的 (参见第 1 章 §4 定理 1 的证明), 而且显然 $\mathrm{Ker}\,\overline{\Phi} = (\mathrm{Ker}\,\Phi)/K$. 特别地, 如果 $K = \mathrm{Ker}\Phi$, 则表示 $\overline{\Phi}$ 是忠实的.

反之, 若有满同态 $\pi: G \to H$, 则群 H 的任一线性表示 Ψ 都诱导一个群 G 的表示 Φ, 这只需令

$$\Phi(g) = \Psi(\pi(g))$$

即可. 因为 π 是满射, 所以 $\Phi(G) = \Psi(H)$ 且 Φ, Ψ 同时可约或不可约. 由对应定理 (第 1 章 §4 定理 3), $\mathrm{Ker}\,\Phi = \pi^{-1}(\mathrm{Ker}\,\Psi)$. 因为交换群 (而准确地, 循环群) $\mathrm{Im}\,\Phi$ 是与群 G 的任一一维表示 Φ 相对应, 所以 $\mathrm{Ker}\,\Phi \supset G'$. 现在由简单地运用定理 3, 上面所做的说明以及第 1 章 §4 定理 4, 就得到定理的证明. □

4. 某些特殊群的表示 虽然原则上讲, 为了得到有限群 G 的所有不可约表示, 只需将它分解为正则表示 (定理 2), 但是实际上这有极大的困难, 必须采用其他迂回的方法. 经常采取的方法是首先建立特征标表, 然后再构造表示本身 (参见第 4 章 §4 相关内容). 不过下面我们有机会见到一些例子都是相当简单, 而不需要任何技巧.

A) 假设 G 是作用在集合 $\Omega = \{1, 2, \cdots, n\}$ 上的任一 2-可迁置换群 (见第 1 章 §3 例 3). 再令 Φ 是群 G 在空间 $V = \langle e_1, e_2, \cdots, e_n\rangle$ 上的一个自然表示, 其作用为 $\Phi(g)e_i = e_{g(i)}$ (见 §1 例 5). 不难理解, 值 $\chi_\Phi(g)$ 等于在 g 作用下保持不变的点 $i \in \Omega$ (基向量 e_i) 的个数 $N(g)$. 根据第 1 章 §3 定理 3, 我们有

$$\sum_{g\in G} \chi_\Phi(g)\overline{\chi_\Phi(g)} = \sum_{g\in G} \chi_\Phi(g)^2 = \sum_{g\in G} N(g)^2 = 2|G|,$$

显然这可以改写为

$$(\chi_\Phi, \chi_\Phi)_G = 2. \tag{5}$$

将 (5) 与 §4 关系式 (11) 对照, 我们得到结论: Φ 是两个不可约表示的直和 ($2 = 1+1$ 是 2 写为自然数平方和的唯一形式). 但是我们也知道, $\Phi = \Phi^{(1)}\dot{+}\Psi$, 其中 $(\Phi^{(1)}, U)$ 是单位表示, 而 Ψ 是作用在空间 $W = \langle e_1 - e_n, e_2 - e_n, \cdots, e_{n-1} - e_n\rangle$ 上的 $n-1$ 维表示. 如果分解式 $V = U \oplus W$ 可以继续在 W 上分解, 那么不可约的项将超过 2. 于是, 我们有下列非平凡的论断.

域 $\mathbb{C}$ 上的 2–可迁置换群的自然的线性表示 (Φ, V) 是一个由单位表示和一个不可约表示的直和.

特别地, 群 $S_n, n > 2; A_n, n > 3$ 中的每一个都有一个 $\mathbb{C}$ 上的 $n-1$ 维的不可约表示 Ψ, 且其特征标 χ_Ψ 由公式

$$\chi_\Psi(g) = N(g) - 1 \tag{6}$$

算出. □

我们曾经作为例子讨论过群 S_3 (§2 第 1 目例 1), 找出矩阵 Ψ_g 也没有特别的困难. 为了由公式 (6) 算出 $\chi_\Psi(g)$, 只要知道置换 g 的循环结构. 少量的图解说明如下:

A_4	e	$(1\ 2)(3\ 4)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
χ_Ψ	3	-1	0	0

S_4	e	$(1\ 2)(3\ 4)$	$(1\ 2)$	$(1\ 2\ 3)$	$(1\ 2\ 3\ 4)$
χ_Ψ	3	-1	1	0	-1

A_5	e	$(1\ 2)(3\ 4)$	$(1\ 2\ 3)$	$(1\ 2\ 3\ 4\ 5)$	$(1\ 2\ 3\ 5\ 4)$
χ_Ψ	4	0	1	-1	-1

B) *交错群 A_4 的不可约表示.* 我们收集一下我们已经知道的一些事实. 群 A_4 有 4 个共轭元素类. 这些类的代表元和它们的势放在下表的上面两行

12	1	3	4	4
A_4	e	$(1\ 2)(3\ 4)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
χ_1	1	1	1	1
χ_2	1	1	ε	ε^{-1}
χ_3	1	1	ε^{-1}	ε
χ_4	3	-1	0	0

换位子群 $A_4' = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ 在 A 中的指数为 3, 所以 A_4 有 3 个一维表示: $\Phi^{(1)} = \chi_1, \Phi^{(2)} = \chi_2, \Phi^{(3)} = \chi_3$ (其核为 A_4' 且 $\varepsilon^3 = 1, \varepsilon \neq 1$), 和一个三维表示 $\Phi^{(4)}(12 = 1^2 + 1^2 + 1^2 + 3^2)$. 与 §4 中例 1 和例 2 中 A_4 的表作比较, 我们

看到, 具有特征标 χ_4 的表示 $\Phi^{(4)}$ 等价于旋转群 A_4 (四面体群) 的表示 Φ, 也等价于群 A_4 的与 2–可迁群 A_4 相联系的表示 Ψ.

C) *对称群 S_4 的不可约表示*. 下表的上两行取自第 1 章 §3 习题 4. 表示 $\Phi^{(1)} =$

24	1	3	6	8	6
S_4	e	(1 2)(3 4)	(1 2)	(1 2 3)	(1 2 3 4)
χ_1	1	1	1	1	1
χ_2	1	1	−1	1	−1
χ_3	2	2	0	−1	0
χ_4	3	−1	−1	0	1
χ_5	3	−1	1	0	−1

χ_1 是单位表示. 表示 $\Phi^{(2)}$ 由 S_4 中置换的奇偶性确定 (正负号). 因为 $(S_4 : S_4') = 2$ (第 1 章 §4 第 2 目例子), 所以再没有其它一维的表示. 具有特征标 χ_3 和核 $V_4 \lhd S_4$ 的二维表示 $\Phi^{(3)}$ 由定理 5 的证明中所叙述的得出. 具有特征标 χ_4 的表示 $\Phi^{(4)}$ 由立方体的旋转得出 (见 §4 例 2 对于 S_4 的表). 带有特征标 χ_5 的表示 $\Phi^{(5)} = \Psi$ (见例 1 中的表) 与群 S_4 的 2–可迁性相联系. 它也等价于适合四面体的所有对称变换 Δ_4 (旋转加反射) 的表示; 也就是说, 这些变换对于描述磷分子的振动是重要的 ([BA I] 第 1 章 §2 问题 2).

D) *四元数群 Q_8 的不可约表示*. 关于四元数群 Q_8 已在第 1 章 §4 第 5 目例 2 中介绍过了. 那里给出了 (但没有说出自己的名称) 具有下列特征标 χ_5 的一个二维不可约表示 $\Phi^{(5)}$;

8	1	1	2	2	2
Q_8	e	a^2	a	b	ab
χ_1	1	1	1	1	1
χ_2	1	1	−1	−1	1
χ_3	1	1	−1	1	−1
χ_4	1	1	1	−1	−1
χ_5	2	−2	0	0	0

四个一维表示有核为换位子群 $\langle a^2\rangle$, 且它们被第 3 段的例子中的表所确定.

习 题

1. 利用不可约特征标, 对于基中心函数 Γ_i (见 §4 (7)) 的分解式 $\Gamma_i = \sum_j t_{ij}\chi_j$ 的系数以明显的式子 $t_{ij} = (\Gamma_i, \chi_j)_G$ 来描绘, 从而得出关系 (4).
2. 证明 (回想一下关于向量空间 V 和与它共轭的线性函数空间 V^* 之间的同构), 由条件 $a^\tau(\chi) = \chi(a)$ 定义的映射 $\tau : A \to \hat{\hat{A}}$ 是交换群 A 到 $\hat{\hat{A}}$ 上的一个同构映射.

这个结论和定理 4 一道建立了所谓的有限交换群的*对偶原理*. 对于拓扑交换群有类似的但要比对偶原理深刻得多的原理, 是由 L.S. 邦特列雅金 (苏) 创立的, 并由此导致了一些重要结果.

3. 证明, 如果有限交换群 A 有忠实的复不可约表示, 那么 A 是一个循环群.

4. 假设 A 是有限交换群, B 是它的子群. 证明, 群 B 的特征标可拓展为群 A 的特征标, 且这样的拓展的个数等于指数 $(A:B)$.

5. 论证第 4 目 C) 中最后括号前的一句话.

6. 复特征标 χ 在有限群 G 的元素上的平均值 $\frac{1}{|G|}\sum_g \chi(g)$ 等于什么?

7. 收集与群 A_5 有关的不同的表, 汇总出下列特征标表:

60 A_5	1 e	15 $(1\ 2)(3\ 4)$	20 $(1\ 2\ 3)$	12 $(1\ 2\ 3\ 4\ 5)$	12 $(1\ 2\ 3\ 5\ 4)$
χ_1	1	1	1	1	1
χ_2	3	-1	0	$(1+\sqrt{5})/2$	$(1-\sqrt{5})/2$
χ_3	3	-1	0	$(1-\sqrt{5})/2$	$(1+\sqrt{5})/2$
χ_4	4	0	1	-1	-1
χ_5	*	*	*	*	*

给出具有特征标 $\chi_1,\chi_2,\chi_3,\chi_4$ 的不可约表示的表述. 并利用特征标的第二正交关系 (4) 填写表格的最后一行.

8. 假设 $P=\langle A^iB^jC^k; 0\leqslant i,j,k\leqslant p-1\rangle$ 是 p^3 阶群, 曾在第 1 章 §3 习题 3 中研究过; $V=\langle e_0,e_1,\cdots,e_{p-1}\rangle_{\mathbb{C}}$ 是 p 维复向量空间; ε 为 1 的 p 次本原根; $\mathcal{A},\mathcal{B},\mathcal{C}$ 是 V 上的线性算子, 其定义关系为

$$\mathcal{A}e_i=e_{i+1},\ \mathcal{B}^ke_i=\varepsilon^{-ki}e_i,\ \mathcal{C}^ke_i=\varepsilon^ke_i,\quad 0\leqslant i\leqslant p-1.$$

(基元的下标按模 p 来取).

证明: 映射

$$\Phi^{(k)}: A\mapsto\mathcal{A},\quad B\mapsto\mathcal{B}^k,\quad C\mapsto\mathcal{C}^k$$

确定了群 P 的一个线性不可约表示. 表示 $\Phi^{(1)},\cdots,\Phi^{(p-1)}$ 两两不等价且与 p^2 个一维表示一起 (p^2 为换位子群 $P'=\langle C\rangle$ 在 P 中的指数) 组成群 P 的所有不可约复表示.

9. 补充计算下列论断. 设

$$D_n=\langle a,b|a^n=e,b^2=e,bab^{-1}=a^{n-1}\rangle$$

是阶为 $2n$ 的二面体群, 它的性质 (包括共轭元素类的描写) 已在第 1 章 §4 第 5 目例 1 中给出. 因为 $\langle a\rangle\lhd D_n$, 所以映射 $a\mapsto 1,b\mapsto 1$ 和 $a\mapsto 1,b\mapsto -1$ 给出两个一维表示. 令 ε 是 1 的 n 次本原根. 那么映射

$$\Phi^{(j)}: a\mapsto\begin{pmatrix}\varepsilon^j & 0\\ 0 & \varepsilon^{-j}\end{pmatrix}$$

将确定一个 2 维表示. 表示 $\Phi^{(j)}$ 在 $j = 1, 2, \cdots, [(n-1)/2]$ 时不可约 (这里 $[a]$ 表示实数 a 的整数部分). 当 $n = 2m$ 时, 表示 $\Phi^{(m)}$ 被分解为两个一维表示 $a \mapsto -1, b \mapsto 1$ 和 $a \mapsto -1, b \mapsto -1$ 的直和. 这与这样的事实一致: 换位子群 D'_{2m} 在 D_{2m} 的指数为 4, 而 $D_{2m}/D'_{2m} \cong Z_2 \times Z_2$. 所有指出的表示不可约且成为二面体群的不可约复表示的全部. 找出表示 $\Phi^{(j)}$ 的实的实现. 以明确的形式指出同构 (等价) $\Phi^{(j)} \approx \Phi^{(k)}, k > m, j \leqslant m$.

10. 晶体群 (见 [BA I] 第 1 章 §2 问题 2). 设 E 是 n 维欧几里得空间, V 是与 E 相伴的具有欧几里特内积的向量空间. 空间 E 的任意运动 d 符合正交线性变换 $\overline{d} \subset \mathrm{O}(n)$, 而且 $\overline{d_1 d_2} = \bar{d}_1 \bar{d}_2$. 设空间的运动群为 D, 如果任意点的 D–轨道是离散的 (没有极限点) 且存在紧集合 $M \subset E$ 满足 $D(M) = \bigcup\limits_{d \in D} d(M) = E$, 那么 D 称为**晶体群**. 根据 Shenflisa-Bieberbach 定理, 晶体群 D 包含 n 个无关仿射移动, 它们在 D 中生成一个正规子群 L, 且 $\overline{D} \cong D/L$ 是一个有限群 (晶体点群). 当 $n = 3$ 时, 所有几何上不同的晶体点群有 32 个. 显然, 它们当中可能有群包含反射 (非正常运动). 由结晶性的条件知道, $\overline{D}$ 中的任意正常旋转用矩阵表示是这样的

$$A = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

其迹 $\mathrm{tr}\, A = 1 + 2\cos\theta \in \mathbb{Z}$. 依据 §3 定理 2 和指出的观点证明, 当 $n = 3$ 时, 没有反射的点晶体群只有循环群 C_1, C_2, C_3, C_4, C_6, 二面体群 D_2, D_3, D_4, D_6, 四面体群 $\mathbf{T}$ 和立方体群 (八面体群) $\mathbf{O}$.

§6 群 SU(2) 和群 SO(3) 的表示

与群 SO(3) 的表示相联系的具体形态是 "物理" 思维的部分. 反映许多物理问题之对称的 SO(3) 的作用从数学角度是有趣的, 其中包括, 它诱导一个在方程 $\Delta f = 0$ 的解空间上的作用, 这里

$$\Delta = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}$$

是拉普拉斯微分算子. 这个问题的二维模型曾在本章开头讨论过 (问题 1).

群 SO(3) 的每个元是形如第 1 章 §1 中 (1) 的某些算子 B_φ, C_θ 的积. 但是 B_φ 不作用在 z 上, 而 C_θ 作用在 x 上. 因此方程 $\Delta f = 0$ 对于 B_φ 和 C_θ 的不变性可由在二维的情形下所得到的计算结果得到. 我们现在得出结论: 方程 $\Delta f = 0$ 对于整个群 SO(3) 是不变的, 或者换句话说,

$$\Delta f = 0 \Longrightarrow \Delta(\Phi_g f) = 0, \quad \forall g \in \mathrm{SO}(3),$$

其中 $\Phi_g f$ 是由关系式

$$(\Phi_g f)(x, y, z) = f(g^{-1}(x), g^{-1}(y), g^{-1}(z)) \tag{1}$$

所定义的函数. 由条件, 对于具有矩阵 $(a_{ij})_1^3$ 的正交变换 g^{-1}, 其新的变量的列有形式

$$\begin{pmatrix} g^{-1}(x) \\ g^{-1}(y) \\ g^{-1}(z) \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

根据 (1)

$$\begin{aligned}(\Phi_g(\Phi_h f))(x,y,z) &= (\Phi_h f)(g^{-1}(x), g^{-1}(y), g^{-1}(z)) \\ &= f(h^{-1}(g^{-1}(x)), h^{-1}(g^{-1}(y)), h^{-1}(g^{-1}(z))) \\ &= f((gh)^{-1}(x), (gh)^{-1}(y), (gh)^{-1}(z)) \\ &= (\Phi_{gh} f)(x,y,z).\end{aligned}$$

于是

$$\Phi_g \Phi_h = \Phi_{gh},$$

也就是说, 线性算子 $\Phi_g, g \in \mathrm{SO}(3)$, 作用在函数上满足映射 $\Phi : g \mapsto \Phi_g$, 是群 SO(3) 的一个表示. 这个很自然的构造表示的方法 (这实际上我们以前在研究带有群 S_n 的作用的对称函数时采用过) 原则上适用于许多群类且它属于常见的泛函分析的方法之列. 仅仅需要依据具体的条件, 选择必要的函数空间, 然后再将其分解为不可约的不变子空间 (调和分析的问题).

假设群 SO(3) 的所有不可约表示是有限维的 (相同的事实对于紧群), 函数取为固定次数 m 的齐次多项式

$$f(x,y,z) = \sum_{s,t} a_{s,t} x^s y^t z^{m-s-t},$$

$(m = 1, 2, 3, \cdots)$. 它们构成 $\begin{pmatrix} m+2 \\ 2 \end{pmatrix}$ 维的空间 P_m (见 [BA I], 第 5 章 §2, 习题 4). 因为 $\Delta f \in P_{m-2}$, 所以条件 $\Delta f = 0$ 等价于在系数 $a_{s,t}$ 上的 $\begin{pmatrix} m \\ 2 \end{pmatrix}$ 个线性条件. 方程 $\Delta f = 0$ 的解 $f \in P_m$ 称为 *m 次齐次调和多项式*. 由于算子 Δ 的线性性, 它们组成维数为 $\begin{pmatrix} m+2 \\ 2 \end{pmatrix} - \begin{pmatrix} m \\ 2 \end{pmatrix} = 2m+1$ 的子空间 H_m (我们有维数 $\leqslant 2m+1$, 但是实际上有等式). 根据上面所说, H_m 对于群 SO(3) 的作用 $\Phi = \Phi^{(m)}$ 是不变的. 于是, 关于下列事实的定理是正确的: *表示 $\Phi^{(m)}$ 的空间 H_m 在 $\mathbb{C}$ 上不可约且群 SO(3) 在 $\mathbb{C}$ 上的任何不可约表示等价于奇维数 $2m+1$ 的表示*$(\Phi^{(m)}, H_m)$ *之一*. 我们不证明这个定理, 而只是交待一下, 并将注意力转到群 SU(2), 这里稍微容易地得到不可约表示的族. 由于存在自然同态 $\mathrm{SU}(2) \to \mathrm{SO}(3)$ 其核由矩阵 $\pm E$ 组成 (见第 1 章 §1), 群 SO(3) 的任意表示 Ψ 同样可以看作为群 SU(2) 的表示 (见 §5 定理 5 的证明), 且满

足称之为奇偶性的条件: $\Psi_{-e}=\Psi_e$. 在这种情况下, 不言而喻, 对于所有 $g\in \mathrm{SU}(2)$, 将同样满足等式 $\Psi_{-g}=\Psi_g$. 反之, 在满足奇偶性条件下, 群 SU(2) 的表示 Ψ 同样是 SO(3) 的表示. 群 SO(3) 的 "双值的" 表示, 即不满足奇偶性条件的群 SU(2) 的表示也具有物理涵义. 例如, 通常的二维 (自旋) 表示属于它们之列.

我们也指出, 群 SO(3) 的不同于单位的任意不可约表示是忠实的, 这可以从群 SO(3) 的单性直接得到 (第 2 章 §1 定理 3).

定理 1 假设 $V_n=\langle x^k y^{n-k}|k=0,1,\cdots,n\rangle_{\mathbb{C}}$ 是一个具有两个复变量的 n 次齐次多项式的空间, 且群 SU(2) 在其上对于每个元素

$$g=\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix},\quad |\alpha|^2+|\beta|^2=1,$$

有作用 $\Psi^{(n)}$:

$$\left(\Psi_g^{(n)}f\right)(x,y)=f(\overline{\alpha}x-\beta y,\overline{\beta}x+\alpha y),$$

则 $(\Psi^{(n)},V_n)$ 是群 SU(2) 的维数为 $n+1$ 的不可约表示. 当 n 是偶数时, $\left(\Psi^{(n)},V_n\right)$ 也是群 SO(3) 的不可约表示.

证明 假设多项式

$$f(x,y)=\sum_{k=0}^{n}a_k x^k y^{n-k}\neq 0$$

包含在某一个不变子空间 $U\subset V_n$ 中. 那么同样

$$\sum_{k=0}^{n}\left(e^{-i\varphi}\right)^k a_k x^k y^{n-k}=e^{-in\varphi/2}\left(\Psi_{b\varphi}^{(n)}f\right)(x,y)\in U,$$

其中 b_φ 是 SU(2) 中形如第 1 章 §1 (4) 的元. 因为 φ 是区间 $(0,2\pi)$ 中的任意实数, 所以可以得出具有范德蒙德行列式的线性系, 由此得到, 对于任意其系数 $a_k\neq 0$ 的单项式,

$$f(x,y)\in U\Longrightarrow x^k y^{n-k}\in U. \tag{2}$$

但是如果对于某个 k 有 $x^k y^{n-k}\in U$, 那么

$$\overline{\alpha}^k\overline{\beta}^{n-k}x^n+\cdots+(\overline{\alpha}x-\beta y)^k(\overline{\beta}x+\alpha y)^{n-k}=\Psi_g^{(n)}\left(x^k y^{n-k}\right)\in U.$$

取 g 具有 $\alpha\beta\neq 0$, 由 (2) 我们有 $x^n\in U$, 而这本身也推出

$$\sum_{s=0}^{n}\binom{n}{s}\overline{\alpha}^s(-\beta)^{n-s}x^s y^{n-s}\in U.$$

因为 $\binom{n}{s}\overline{\alpha}^s(-\beta)^{n-s}\neq 0$, 所以 $x^s y^{n-s}\in U, s=0,1,\cdots,n$. 于是 $U=V_n$, 从而 $\left(\Psi_n^{(n)},V_n\right)$ 的不可约性被证明了.

其次

$$\Psi_e^{(n)}\left(x^k y^{n-k}\right)=(-x)^k\left(-y^{(n-k)}\right)=(-1)^n x^k y^{n-k},$$

所以当 $n=2m$ 时它满足奇偶性条件 (见上面的说明) 且 $(\Psi^{(2m)}, V_{2m})$ 可以认为是 $2n+1$ 维的不可约表示. □

实际上, $\Psi^{(2m)}$ 等价于群 SO(3) 在 m 次齐次调和多项式空间上的表示 $\Phi^{(m)}$, 但是我们不在此停留, 也不打算 (虽然这是可能的) 在 V_n 中选择那样的基, 使得表示 $\Psi^{(n)}$ 成为酉表示. 我们仅仅指出, 借用张量分析的术语, 群 SU(2) 的表示 $\Psi^{(n)}$ 同样可以在 n 级共变对称张量类中实现. 紧群 (包括 SU(2) 和 SO(3)) 的完整也十分易懂的表示理论通常借助于李群和李代数的对应关系在无穷小方法的范围内发展. 关于这一点在第 2 章已多少谈过.

习 题

1. 构造 $2m+1$ 个线性无关的 m 次齐次调和多项式.
2. 证明: 任意齐次多项式 $f\in P_m$ 可以写为次数为 $m, m-2, m-4,\cdots$ 的调和多项式的线性组合, 其系数依赖于 $x^2+y^2+z^2$.
3. 由习题 2 得出: 球面 $S^2: x^2+y^2+z^2=1$ 上的任一多项式函数 $\widetilde{g}:(X,Y,Z)\mapsto g(x,y,z)$ 能够按球面函数 (调和函数在 S^2 上的限制) 来分解.
4. 不通过群 SO(3) 的不可约表示的完全描写, 证明同态 $\tau: \mathrm{SO}(3)\to\mathrm{SU}(2)$ 也许只是平凡的.

§7 表示的张量积

1. 逆步表示 假设 (Φ, V) 是群 G 在域 $\mathbb{C}$ 上的一个表示. 我们来看对偶空间 V^* (即 V 上的线性函数的空间) 且令

$$(\Phi^*(g)f)(v)=f\left(\Phi(g^{-1})v\right),\quad f\in V^*, v\in V. \tag{1}$$

算子 $\Phi^*(g)$ 的线性性可立即验证. 在 V 和 V^* 中选取对偶基:

$$V=\langle e_1,\cdots,e_n\rangle,\ V^*=\langle f_1,\cdots,f_n\rangle,\quad f_i(e_j)=\delta_{ij}.$$

线性算子 $\Phi^*(g)$ 在基 $(f_1,\cdots,f_n)$ 上的矩阵是算子 $\Phi(g^{-1})$ 在基 $\langle e_1,\cdots,e_n\rangle$ 上矩阵的转置矩阵:

$$\Phi_g^*={}^t\Phi_{g^{-1}}. \tag{2}$$

因为

$$\Phi_{gh}^*={}^t\Phi_{(gh)^{-1}}={}^t\Phi_{h^{-1}g^{-1}}={}^t(\Phi_{h^{-1}}\Phi_{g^{-1}})={}^t\Phi_{g^{-1}}{}^t\Phi_{h^{-1}}=\Phi_g^*\Phi_h^*,$$

所以, 一般地讲, 关系 (2) (或 (1)) 所确定的是群 G 的新的线性表示 (Φ^*, V^*); 它被称为表示 (Φ, V) 的逆步 (或对偶) 表示. 每当我们令作用在向量 (反变张量) 上的群作用到向量的坐标 (共变张量) 上时 (实际上这已在 §6 出现过), 研究这种表示的必要性都将出现. 由 (2) 不难发现, $(\Phi^*)^* \approx \Phi$. 互相逆步的表示也许没有区别或者等价. 例如, 如果 (Φ, G) 是一个实正交表示, 那么 $\Phi_g^* = {}^t\Phi_{g^{-1}} = \Phi_g$. 但在一般情况下, 表示 Φ 与 Φ^* 是不等价的, 最简单的例子是:

$$C_3 = \langle a | a^3 = e \rangle; \quad \Phi(a) = \varepsilon, \quad \Phi^*(a) = \varepsilon^{-1} \quad (\varepsilon^3 + \varepsilon + 1 = 0).$$

对于有限群 G, 逆步表示的等价性的准确的判别准则可用特征标理论的语言得到. 因为矩阵 A 与 ${}^tA$ 的特征多项式相等, 所以由特征标的初等性质 (见 §4) 推出

$$\chi_{\Phi^*}(g) = \overline{\chi_\Phi(g)}.$$

特别地, 特征标仅为实数值的表示 Φ 等价于 Φ^*. 自然地总有

$$(\chi_{\Phi^*}, \chi_{\Phi^*})_G = (\chi_\Phi, \chi_\Phi)_G,$$

于是 Φ^*, Φ 同时可约或不可约.

2. 表示的张量积 在 [BA II] 中已经定义和构造了域 P 上的任意两个向量空间 V 和 W 的张量积. 同样线性算子 $\mathcal{A}: V \to V, \mathcal{B}: W \to W$ 的张量积

$$\mathcal{A} \otimes \mathcal{B}: V \otimes W \to V \otimes W$$

也曾被定义. 它是这样定义的:

$$\mathcal{A} \otimes \mathcal{B}(v \otimes w) = \mathcal{A}v \otimes \mathcal{B}w, \tag{3}$$

而由线性性, 我们有

$$(\mathcal{A} \otimes \mathcal{B}) \left(\sum_{i,j} v_i \otimes w_j \right) = \sum_{i,j} \mathcal{A}v_i \otimes \mathcal{B}w_j.$$

由定义 (3) 不难推得下列关系

$$\begin{aligned}
&(\mathcal{A} \otimes \mathcal{B})(\mathcal{C} \otimes \mathcal{D}) = \mathcal{AC} \otimes \mathcal{BD}, \\
&(\mathcal{A} + \mathcal{C}) \otimes \mathcal{B} = \mathcal{A} \otimes \mathcal{B} + \mathcal{C} \otimes \mathcal{B}, \\
&\mathcal{A} \otimes (\mathcal{B} + \mathcal{D}) = \mathcal{A} \otimes \mathcal{B} + \mathcal{A} \otimes \mathcal{D}, \\
&\mathcal{A} \otimes \lambda\mathcal{B} = \lambda\mathcal{A} \otimes \mathcal{B} = \lambda(\mathcal{A} \otimes \mathcal{B}),
\end{aligned}$$

同时对于迹有公式

$$\mathrm{tr}\mathcal{A} \otimes \mathcal{B} = \mathrm{tr}\mathcal{A} \cdot \mathrm{tr}\mathcal{B}. \tag{4}$$

现在假设 $(\Phi, V), (\Psi, W)$ 是群 G 的分别带有特征标 χ_Φ, χ_Ψ 的两个线性表示. 自然地我们定义表示 $(\Phi\otimes\Psi, V\otimes W)$ 的像:

$$(\Phi\otimes\Psi)(g) = \Phi(g)\otimes\Psi(g), \quad \forall g\in G.$$

由线性算子张量积的一般性质和公式 (4) 知, 映射 $\Phi\otimes\Psi$ 将确实给出群 G 的具有表示空间 $V\otimes W$ 和特征标

$$\chi_{\Phi\otimes\Psi} = \chi_\Phi\chi_\Psi \tag{5}$$

的一个表示. 我们称 $(\Phi\otimes\Psi, V\otimes W)$ 为表示 (Φ, V) 和 (Ψ, W) 的*张量积*. 当 $\Psi = \Phi, W = V$ 时, 同样称为*张量的平方*. 等式 (5) 的右边是中心函数 χ_Φ 和 χ_Ψ 的通常的逐项积.

十分显然, 如果 U 是 V 中的 G–不变子空间, 那么 $U\otimes W$ 也是 $V\otimes W$ 中的 G–不变子空间. 类似的结论对于 W 中的 G–不变子空间也成立. 但是, 由 V 和 W 的不可约性决不会推出 $V\otimes W$ 的不可约性, 例如群 S_3 的二维表示的张量积 $\Phi^{(3)}\otimes\Phi^{(3)}$ (见 §5 第 2 目中的表). 实际上, $\dim_{\mathbb{C}}\Phi^{(3)}\otimes\Phi^{(3)} = 4$, 而群 S_3 的不可约表示的最大维数等于 2.

包含在 $\Phi\otimes\Psi$, 或一般地, 包含在一些线性表示的张量积

$$\Phi^{(1)}\otimes\Phi^{(2)}\otimes\cdots\otimes\Phi^{(p)}$$

中的不可约表示的有效描写的问题有重要的意义, 因为许多重要的且非常自然的群表示都以张量积的形式出现. 正是从这个角度需要来考察群 SU(2) 和群 SO(3) 的表示 (见 §6), 同样需要来考察 §1 第 2 目的例 3 和例 4. 对称和斜对称的共变 (或反变) 张量的不变子空间常常出现在各种几何应用中. 当表示的完全可约性的定理成立时, 所考虑的问题尤其诱人.

3. 特征标环 为了简便起见, 我们只讨论复数域 $\mathbb{C}$ 上有限群 G 的情形. 假设 $\Phi^{(1)}, \Phi^{(2)}, \cdots, \Phi^{(r)}$ 是 $\mathbb{C}$ 上群 G 的两两不等价的不可约表示, $\chi_1, \chi_2, \cdots, \chi_r$ 为它们相应的特征标 (r 为 G 中共轭元素类的个数). 我们知道,

$$\Phi\otimes\Psi \approx m_1\Phi^{(1)}\dot{+}m_2\Phi^{(2)}\dot{+}\cdots\dot{+}m_r\Phi^{(r)},$$

其中重数 m_i 仅取决于 Φ 和 Ψ. 由公式 (5)

$$\chi_\Phi\chi_\Psi = m_1\chi_1 + \cdots + m_r\chi_r.$$

设 $X_{\mathbb{Z}}(G)$ 为特征标 $\chi_1, \cdots, \chi_r$ 的所有可能的整数线性组合的集合. 我们以前证明过, $(\chi_1, \cdots, \chi_r)$ 是空间 $X_{\mathbb{C}}(G)$ 的标准正交基, 因此 $X_{\mathbb{Z}}(G)\subset X_{\mathbb{C}}(G)$ 在任何情况下是具有生成元 $\chi_1, \cdots, \chi_r$ 的一个自由交换群, 它 $\cong \mathbb{Z}^r$. 它的元素称为群 G 的**广义特征标**. 这些组合 $\sum m_i\chi_i, m_i\geqslant 0$, 将是仅有的真正的特征标.

由前面的讨论看到, 表示的张量积在 $X_{\mathbb{Z}}(G)$ 上诱导一个二元代数运算, 这个运算适合交换律、结合律和分配律. 简言之, 下列定理成立.

定理 1 广义特征标构成一个有单位元的交换结合环 $X_{\mathbb{Z}}(G)$, 其单位元是单位特征标 χ_1.

$X_{\mathbb{C}}(G)$ 本身也是一个 $\mathbb{C}$ 上的 r 维的交换结合代数. 环 $X_{\mathbb{C}}(G)$ (代数 $X_{\mathbb{C}}(G)$) 的结构完全由构造常数, 即关系式

$$\chi_i\chi_j = \sum_k m_{ij}^k \chi_k \tag{6}$$

中的整数 m_{ij}^k, 所确定. 特别地, 等式 $m_{ij}^k = m_{ji}^k, m_{1j}^k = \delta_{kj}$ 反映了 $X_{\mathbb{Z}}(G)$ 的可换性和 χ_1 的单位性. 由 (6)

$$\chi_i(g)\chi_j(g) = \sum_k m_{ij}^k \chi_k(g), \quad \forall g \in G.$$

在此式两边同乘 $\frac{1}{|G|}\overline{\chi_s(g)}$, 按 $g \in G$ 求和并应用特征标的第一正交关系, 我们得到

$$m_{ij}^s = \frac{1}{|G|}\sum_{g\in G} \chi_i(g)\chi_j(g)\overline{\chi_s(g)}. \tag{7}$$

于是, 构造常数表达为特征标的术语.

由 (7) 可以得到一个不复杂的论断:

$$\begin{aligned} m_{ij}^1 &= \frac{1}{|G|}\sum_g \chi_i(g)\chi_j(g)\overline{\chi_1(g)} = \frac{1}{|G|}\sum_g \chi_i(g)\chi_j(g) \\ &= \frac{1}{|G|}\sum_g \chi_i(g)\overline{\overline{\chi_j(g)}} = (\chi_i, \chi_j^*)_G, \end{aligned}$$

其中 $\chi_j^* = \chi_\Psi, \Psi = \Phi^{(j)*}$ 是 $\Phi^{(j)}$ 的逆步表示 (见第 1 目) 的特征标. 于是, 单位表示能作为分量出现在 $\Phi^{(i)} \otimes \Phi^{(j)}$ 的分解式中当且仅当 $\Phi^{(i)}$ 等价于表示 $\Phi^{(j')} = \Phi^{(j)*}$ (否则 $m_{ij}^1 = (\chi_i, \chi_j^*)_G = 0$). 我们也指出, 一维表示 $\Phi^{(i)}$ 与任意不可约表示 $\Phi^{(j)}$ 的张量积总是不可约表示, 其维数为 $\Phi^{(j)}$ 的维数. 这是相当明显的, 不需要任何解释, 而正式地可由不可约特征标的检验得出. 如果

$$\chi = \chi_{\Phi^{(i)}\otimes\Phi^{(j)}} = \chi_i\chi_j,$$

那么 $\chi_i(g)$ 是它的次数为 1 的复根且 $\chi_i(g)\overline{\chi_i(g)} = 1$, 所以

$$\begin{aligned} (\chi, \chi)_G &= \frac{1}{|G|}\sum_g \chi_i(g)\chi_j(g)\overline{\chi_i(g)\chi_j(g)} \\ &= \frac{1}{|G|}\sum_g \chi_j(g)\overline{\chi_j(g)} = (\chi_j, \chi_j)_G = 1. \end{aligned}$$

例 1 $G = S_3$ (见 §2 第 1 目的表及 §5 第 2 目中的表):

$$\Phi^{(1)} \otimes \Phi^{(3)} \approx \Phi^{(2)} \otimes \Phi^{(3)} \approx \Phi^{(3)}.$$

例 2 $G = S_4$ (见 §5 第 4 目例 3):

$$\Phi^{(2)} \otimes \Phi^{(4)} \approx \Phi^{(5)} \quad \Phi^{(2)} \otimes \Phi^{(5)} \approx \Phi^{(4)}.$$

最后我们来证明下列有趣的定理, 它是 §5 中关于正则表示分解的定理 2 的推广.

定理 2 假设 $\chi = \chi_\Phi$ 是复数域 $\mathbb{C}$ 上有限群 G 的忠实表示 (Φ, V) 的特征标, 它在 G 上有 m 个不同的值. 那么每一个不可约特征标 χ_k 带有非零系数地包含在特征标 $\chi^0 = \chi_1, \chi, \chi^2, \cdots, \chi^{m-1}$ 至少某一个的分解中. 换句话说, 对于任意忠实表示 Φ, 每一个不可约表示包含在某一个张量积 $\Phi^{\otimes^i} = \Phi \otimes \cdots \otimes \Phi, 0 \leqslant i \leqslant m-1$ 的分解中.

证明 假设 $\omega_j = \chi(g_j), j = 0, 1, \cdots, m-1$, 是群 G 上所取的特征标的不同的值, 而且 $\omega_0 = \deg \Phi$. 再令

$$G_j = \{g \in G | \chi(g) = \chi(g_j) = \omega_j\}.$$

根据表示 Φ 的忠实性, 我们有

$$G_0 = \mathrm{Ker}\Phi = \{e\}.$$

假设 χ_k 是不含于任何一个特征标 χ^i 的分解式中的群 G 的不可约特征标. 那么

$$\begin{aligned} 0 &= |G|(\chi^i, \chi_k)_G \\ &= \sum_{j=0}^{m-1} (\chi(g_j))^i \sum_{g \in G_j} \overline{\chi_k(g)} = \sum \omega_j^i T_j, \quad 0 \leqslant i \leqslant m-1, \end{aligned}$$

是相对于

$$T_j = \sum_{g \in G_j} \overline{\chi_k(g)}$$

的齐次线性方程组, 其行列式为

$$\det\left(\omega_j^i\right) = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \omega_0 & \omega_1 & \cdots & \omega_{m-1} \\ \cdots & \cdots & \cdots & \cdots \\ \omega_0^{m-1} & \omega_1^{m-1} & \cdots & \omega_{m-1}^{m-1} \end{vmatrix},$$

它是不等于零的 (因为这是范德蒙德行列式). 于是, $T_j = 0, j = 0, 1, \cdots, m-1$, 即

$$\sum_{g \in G_j} \chi_k(g^{-1}) = 0, \quad j = 0, 1, \cdots, m-1.$$

特别地,

$$0 = \sum_{g \in G_0} \chi_k(g^{-1}) = \chi_k(e).$$

这个矛盾表明定理成立. □

在正则表示 ρ 的情况下, 显然, $m = 2$.

4. 线性群的不变量 令 P 为一个域. 群 $\mathrm{GL}(n, P)$ 的任意子群通常称为 n 级线性群. 以后可以认为 $P = \mathbb{R}$ 或 $P = \mathbb{C}$. 如果 G 是一个抽象群且 $\Phi : G \to \mathrm{GL}(n, \mathbb{C})$ 是 G 的一个线性表示, 那么 (G, Φ) 也将称为线性群. 线性变换 Φ_g 作用在元素 $x_1, \cdots, x_n$ 的列上:

$$\begin{pmatrix} \Phi_g(x_1) \\ \vdots \\ \Phi_g(x_n) \end{pmatrix} = \Phi_g \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

它们将任一 m 次型 (齐次多项式) f 仍变为 m 次型:

$$\left(\widetilde{\Phi}_g f\right)(x_1, \cdots, x_n) = f(\Phi_{g^{-1}}(x_1), \cdots, \Phi_{g^{-1}}(x_n)).$$

这种作用的各种个别情形我们已经见过 (见 §6). 映射 $\widetilde{\Phi}$ 定义了群 G 在复数域 $\mathbb{C}$ 上 m 次型的空间 P_m (或称秩为 m 的共变对称张量空间) 上的一个表示.

定义 在 $\widetilde{\Phi}_g$ 作用下保持不变 (即 $\widetilde{\Phi}_g f = f, \forall g \in G$) 的型 $f \in P_m$ 称为线性群 (G, Φ) 的 m 次 **(完全) 不变型**.

事实上, 我们需要选择在 $\widetilde{\Phi}(G)$ 作用下保持不变的带有系数的 m 次 "一般" 型的多项式. 这样就进入一般的不变理论, 但是为了简便起见, 我们只限于所给的定义. 如果将 f 取为有理函数, 那么可以得到**有理不变**的概念. 同样重要的是 f 的**相对不变** 的概念, 即当

$$\widetilde{\Phi}_g f = \omega_g f,$$

这里 $\omega_g \in \mathbb{C}$ 是取决于元素 $g \in G$ 的一个因子.

显然, 线性群 (G, Φ) 的不变的任一集合 $\{f_1, f_2, \cdots\}$ 在 $\mathbb{C}[x_1, \cdots, x_n]$ 中生成一个不变子环 $\mathbb{C}[f_1, f_2, \cdots]$.

我们来看一些例子.

例 3 二次型 $x_1^2 + x_2^2 + \cdots + x_n^2$ 及它的任意多项式对于正交群 $\mathrm{O}(n)$ 是完全不变的.

例 4 初等对称多项式 $s_1(x_1,\cdots,x_n),\cdots,s_n(x_1,\cdots,x_n)$, 将其看作一个有自然单同态 $\Phi: S_n\to \mathrm{GL}(n,\mathbb{R})$ 的对称群 S_n, 是完全不变的. 对称多项式的基本定理使我们确信, 次数分别为 $1,2,\cdots,n$ 的不变量 $s_1,\cdots,s_n$ 是代数无关的, 而它们的多项式 (有理) 函数穷尽了群 (S_n,Φ) 的所有整 (有理) 的不变量.

斜对称多项式是线性群 (S_n,Φ) 的相对不变量: $\Phi_\pi f=(\det\Phi_\pi)f=\varepsilon_\pi f$. 我们曾看到 ([BA I], 第 6 章 §2 习题 4), 任意斜对称多项式 f 有形式 $f=\Delta_n\cdot g$, 其中 $\Delta_n=\prod\limits_{j<i}(x_i-x_j)$, 而 g 是任意对称多项式, 即绝对不变量.

例 5 n 个代数无关的不变量系 (即矩阵 $X=(x_{ij})$ 的特征多项式的系数) 适合具有表示空间 $M_n(K)$ (见 §1 例 3) 的完全线性群 $\mathrm{GL}(n,K)$ 的 n^2 级表示 $\Phi_A: X\mapsto AXA^{-1}$. 其中包括我们非常熟悉的与它们有关的不变量 $\mathrm{tr}X=\sum\limits_i x_{ii}$ 和 $\det X$.

例 6 设二次型

$$f=(x_1,\cdots,x_n)=\sum a_{ij}x_ix_j,$$

将它改写为下列形式

$$f(x_1,\cdots,x_n)={}^tXAX;\ \text{其中}\ A=(a_{ij})={}^tA,\quad X=[x_1,\cdots,x_n],$$

正交群 $\mathrm{O}(n)$ 作用在该二次型上:

$$\begin{aligned}C\in\mathrm{O}(n)\Longrightarrow(C^{-1}f)(x_1,\cdots,x_n)&={}^t(CX)A(CX)\\&={}^tX{}^tCACX={}^tX({}^tCAC)X.\end{aligned}$$

在这种情形可以谈论关于 $\mathrm{O}(n)$ 的二次型 f 的不变量: $\mathrm{tr}\,A,\cdots,\det A$. 对于二元二次型 $ax^2+2bxy+cy^2$, 不变量是 $a+c$ 和 $ac-b^2$, 它们刻画了不同的二阶曲线类的度量, 这在解析几何教程也是知道的.

例 7 利用表示 Γ, 它等价于 §2 第 1 目末表中的 $\Phi^{(3)}$:

$$\Gamma_{(1\ 2\ 3)}=\begin{pmatrix}\varepsilon&0\\0&\varepsilon^{-1}\end{pmatrix},\Gamma_{(2\ 3)}=\begin{pmatrix}0&1\\0&1\end{pmatrix},$$
$$\varepsilon^2+\varepsilon+1=0.$$

其等价性借助于共轭

$$\begin{pmatrix}\varepsilon&0\\0&1\end{pmatrix}\Phi_\sigma^{(3)}\begin{pmatrix}\varepsilon^{-1}&0\\0&1\end{pmatrix}=\Gamma_\sigma,$$

我们将对称群 S_3 看作 2 阶线性群.

设 u,v 是无关的变量, 它们通过 Γ_σ:

$$\Gamma_{(1\ 2\ 3)}(u)=\varepsilon u,\quad \Gamma_{(1\ 2\ 3)}(v)=\varepsilon^{-1}v;$$
$$\Gamma_{(2\ 3)}(u)=v,\qquad \Gamma_{(2\ 3)}(v)=u$$

而被线性变换.

因为

$$\widetilde{\Gamma}_{(1\ 2\ 3)}(uv) = \Gamma^{-1}_{(1\ 2\ 3)}(u)\Gamma^{-1}_{(1\ 2\ 3)}(v) = \varepsilon^{-1}u \cdot \varepsilon v = uv,$$
$$\widetilde{\Gamma}_{(2\ 3)}(uv) = vu = uv,$$
$$\widetilde{\Gamma}_{(1\ 2\ 3)}(u^3+v^3) = (\varepsilon^{-1}u)^3 + (\varepsilon v)^3 = u^3+v^3,$$
$$\widetilde{\Gamma}_{(2\ 3)}(u^3+v^3) = v^3+u^3 = u^3+v^3,$$

所以群 (S_3, Γ) 有二次型和三次型

$$I_1 = uv, \quad I_2 = u^3+v^3 \tag{8}$$

作为自己的不变量.

又, 群 S_3 用自然像的方法作用在三个无关不变量的多项式 $f(x_1, x_2, x_3)$ 上:

$$(\sigma f)(x_1, x_2, x_3) = f(x_{\sigma 1}, x_{\sigma 2}, x_{\sigma 3}).$$

令

$$\begin{aligned} u &= x_1 + \varepsilon^2 x_2 + \varepsilon x_3, \\ v &= x_1 + \varepsilon x_2 + \varepsilon^2 x_3, \end{aligned} \tag{9}$$

我们看到

$$\Gamma_\sigma(u) = x_{\sigma 1} + \varepsilon^2 x_{\sigma 2} + x_{\sigma 3}.$$

特别地,

$$\Gamma_{(1\ 2\ 3)}(u) = x_2 + \varepsilon^2 x_3 + \varepsilon x_1 = \varepsilon u,$$
$$\Gamma_{(2\ 3)}(u) = x_1 + \varepsilon^2 x_3 + \varepsilon x_2 = v,$$
$$\Gamma_{(1\ 2\ 3)}(v) = x_2 + \varepsilon x_3 + \varepsilon^2 x_1 = \varepsilon^{-1} v,$$
$$\Gamma_{(2\ 3)}(v) = x_1 + \varepsilon x_3 + \varepsilon^2 x_2 = u,$$

即, Γ_σ 作用在 u, v 上与 σ 作用在 x_1, x_2, x_3 上一致. 在 (8) 中代入 (9) 得到 x_1, x_2, x_3 的对称函数, 根据 [BA I] 第 6 章 §2 定理 1 知, 它们可以通过初等对称函数 $\mathrm{s}_i = \mathrm{s}_i(x_1, x_2, x_3)$ 来表示. 不难验证

$$I_1 = x_1^2 + x_2^2 + x_3^2 + (\varepsilon + \varepsilon^2)(x_1x_2 + x_1x_3 + x_2x_3) = \mathrm{s}_1^2 - 3\mathrm{s}_2,$$
$$\begin{aligned} I_2 &= 2(x_1^3 + x_2^3 + x_3^3) - 3(x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2) + 12x_1x_2x_3 \\ &= 2\mathrm{s}_1^3 - 9\mathrm{s}_1\mathrm{s}_2 + 27\mathrm{s}_3. \end{aligned}$$

为了得到 I_1, I_2 的特殊的值, 将 x_1, x_2, x_3 作为下列三次方程的根

$$x^3 + px + q = 0.$$

则 $\mathrm{s}_1 = 0, \mathrm{s}_2 = p, \mathrm{s}_3 = -q$, 从而

$$I_1 = -3p, \quad I_2 = -27q. \tag{10}$$

但是由 (8) 我们有

$$v = \frac{I_1}{u}, \quad I_2 = u^3 + \frac{I_1^3}{u^3}, \quad u = \sqrt[3]{\frac{I_2}{2} \pm \sqrt{\frac{I_2^2}{4} - I_1^3}}.$$

将 (10) 代入得到

$$\begin{aligned} u &= \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}}, \\ v &= \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}}, \\ uv &= -3p, \end{aligned}$$

其中 $D = -4p^3 - 27q^2$ 为三次方程的判别式 (见 [BA I] 第 6 章 §2 公式 (16)). 因为 u, v 现在是已知数, 所以由线性方程组

$$\begin{aligned} x_1 + \varepsilon^2 x_2 + \varepsilon x_3 &= u, \\ x_1 + \varepsilon x_2 + \varepsilon^2 x_3 &= v, \\ x_1 + x_2 + x_3 &= 0 \end{aligned}$$

可以解出根. 我们利用相当自然的方法得到了卡尔达诺 (Cardano G.) 公式. 关于卡尔达诺公式已在 [BA I] 第 1 章 §2 问题 1 中得到.

最末的例子绝非偶然地建立了群 S_3 的不变量与卡尔达诺公式之间的联系 (S_3 是一般三次方程的伽罗瓦群). 伽罗瓦理论在很大程度上与研究由代数方程的根生成的域的不变量 (和相应于它们的群) 有联系.

我们将看到与不变量环形成的系统有关的某些事实. 设 w 是 n 个无关变量 $x_1, \cdots, x_n$ 的任意型. 具有 n 维线性表示 Φ 的有限群作为置换群作用在集合

$$\Omega = \{\overline{\Phi}_g(w) | g \in G\}$$

上. 显然 Ω 中 $|G|$ 个元 (或者, 可能, 某一整除 $|G|$ 的因子) 的任意齐次对称函数是线性群 (G, Φ) 不变量. 如果现在取变量 x_i 作为 w, 那么 x_i 将是代数方程

$$\prod_{g \in G} (X - \Phi_g(x_i)) = 0$$

的根, 该方程的系数是群 (G, Φ) 的不变量. 于是, 每个变量 x_i 是不变量的 (代数) 函数. 要是代数无关的变量少于 n 的话, 那么我们就可以用较少的代数无关变量来表示 $x_1, \cdots, x_n$, 而这是不可能的. 因此, 我们证明了不变量的重要定理之一.

定理 3 有限 n 阶线性群总有出自 n 个代数无关的不变量的系.

对于群 (S_3, Γ), 型 (7) 就是这样的不变量.

下列论点也许能补充定理 3: n 阶有限群的完全不变量的整个环由 n 个代数无关不变量 $f_1, f_2, \cdots, f_n$ 和通常再加上一个不变量 f_{n+1} (它是前面 n 个不变量的代数函数) 生成. 换句话说, 所有其余的不变量是 $f_1, \cdots, f_n, f_{n+1}$ 的多项式. 这个事实对于许多其它的线性群都是正确的, 譬如, 离散群和连续群.

不变量的一般理论, 在 19 世纪中叶由于凯莱 (Caylay), 西尔维斯特 (Sylveste)、雅可比 (Jacobi)、埃尔米特 (Hermite)、克莱布施 (Clebsch)、戈丹 (Gordan) 以及其它学者的工作成果而发展起来, 随后由于希尔伯特 (Hilbert) 的一些有重大价值的工作经历了再生. 在今天, 它已经成为代数几何和代数群论的一部分. 同样, 由于它在力学和物理学的许多领域有着广泛的应用, 也决定了不变量理论一直令人引起兴趣.

习 题

1. 利用公式 (6) 和在 §2 第 1 目, §5 第 2 目和 §5 第 4 目中的表, 验证下列分解的正确性:

a) 对于对称群 S_3 的二维表示 $\Phi^{(3)}$ 的张量平方, 有

$$\Phi^{(3)} \otimes \Phi^{(3)} \approx \Phi^{(1)} \dotplus \Phi^{(2)} \dotplus \Phi^{(3)};$$

b) 对于四元数群 Q_8 的二维表示 $\Phi^{(5)}$ 的张量平方, 有

$$\Phi^{(5)} \otimes \Phi^{(5)} \approx \Phi^{(1)} \dotplus \Phi^{(2)} \dotplus \Phi^{(3)} \dotplus \Phi^{(4)}.$$

2. 群的直积表示. 假设 G, H 是两个群, 并分别具有线性表示 $(\Phi, V), (\Psi, W)$. 那么, 令

$$(\Phi \otimes \Psi)(g \cdot h) = \Phi(g) \otimes \Psi(h),$$

其中 $g \cdot h$ 是群 G 和 H 的直积 $G \times H$ 的元, 这样就让 $G \times H$ 作用在张量积 $V \otimes_{\mathbb{C}} W$ 上; 和通常一样,

$$(\Phi(g) \otimes \Psi(h))(v \otimes w) = \Phi(g)v \otimes \Psi(h)w.$$

验证, 这样定义的映射

$$\Phi \otimes \Psi : G \times H \to \mathrm{GL}(V \otimes W)$$

是群 $G \times H$ 的具有特征标 $\chi_{\Phi\otimes\Psi} = \chi_\Phi \chi_\Psi$ 的表示. 证明下列断言: 假设 $\Phi^{(1)}, \cdots, \Phi^{(r)}$ (相应地 $\Psi^{(1)}, \cdots, \Psi^{(s)}$) 是群 G (相应地 H) 的所有不可约表示. 那么群 $G \times H$ 的表示 $\Phi^{(i)} \otimes \Psi^{(j)}$ 不可约, 且群 $G \times H$ 的所有不可约表示也只限于

$$\Phi^{(i)} \otimes \Psi^{(j)}, \quad 1 \leqslant i \leqslant r, \quad 1 \leqslant j \leqslant s.$$

3. 型 $xy, x^n + y^n$ 是二维线性二面体群

$$(D_n, \Phi) = \left\langle \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle, \quad \varepsilon^n = 1$$

的不变量 (见 §5 习题 9). 证明: 群 (D_n, Φ) 的任意其它 (整的) 不变量为 $xy, x^n + y^n$ 的多项式形式.

4. 验证. 四元数群, 在它自己的二维不可约表示中来考察, 没有二次的和三次的不变量. 关于 $x^2y^2, x^4 + y^4$ 怎么样呢?

第 4 章　环. 代数. 模

重新又来考察早先已经研究过的代数结构是出于以下的考虑. 第一, 希望凭借坚实的群论基础在一定程度上补充内容丰富的论断以充实我们关于域和环的知识. 其次, 第 3 章中关于群表示的结果是自然地被包含在环上模的一般理论中的, 但可惜关于这一点, 即使以简短的形式以前也没有提到过. 模的概念本身本来就是重要的并且值得在远为广泛的方面加以研究. 不过, 关于这方面的内容, 我们只向读者推荐一些其它的文献.

§1 环论构造

1. 环的理想及商环　在 [BA I] 第 4 章 §3 中考察过的剩余类环及环的同态为引进一般概念打下了充分好的基础. 我们回想起, 同态

$$f:(K,+,\cdot)\longrightarrow(K',\oplus,\odot)$$

的核是指子环 $\operatorname{Ker}f=\{a\in K|f(a)=0'\}\subseteq K$. 直接明显地看出, 它绝对不是任意的一个子环. 实际上, 如果 $J=\operatorname{Ker}f\subset K$, 则 $J\cdot x\subseteq J$ (这是因为 $f(zx)=f(z)\odot f(x)=0'\odot f(x)=0'$ 对所有 $z\in J$) 且 $x\cdot J\subseteq J$ 对所有 $x\in K$. 因此, $JK\subset J$ 且 $KJ\subset J$. 具有这些性质的子环叫做环 K 的 (双边) 理想. 因此, 同态的核总是理想.

$m\mathbb{Z}\subset\mathbb{Z}$ 这一例子指出了在任意交换环 K 中构造理想 (可能并不是全部的理想) 的方法: 若 a 是 K 中任意一个元素, 则集合 aK 恒是 K 的一个理想. 事实上,

$$ax+ay=a(x+y),(ax)y=a(xy).$$

称 aK 是元素 $a\in K$ 生成的**主理想**.

如果只取含单位元的环, 则理想就是对于用环中元素从左边来乘和从右边来乘都封闭的环的加法群的子群, 而在同态 $f: K \to K'$ 的定义中引入条件 $f(1) = 1'$ 是合适的. 在满同态的情形, 这个条件当然是自动满足的.

在第 1 章中引入的群的正规子群, 和环的理想有共同的来历. 它们都是同态的核. 这种情况也在商结构的构造的共同性方面有它的表述. 我们准备简略地谈一谈.

当构造环 K 对于理想 J 的商环K/J 时, 我们将从环的 "基础" 是加法交换群这一点出发. 因此, 作为 K/J 的元素应该取陪集 $a + J$ (叫做**模理想 J 的剩余类**), 其加法按通常的规则进行:

$$\begin{aligned}(a+J) \oplus (b+J) &= (a+b)+J,\\ \ominus(a+J) &= -a+J.\end{aligned} \tag{1}$$

作为这些类的积, 我们取

$$(a+J) \odot (b+J) = ab + J. \tag{2}$$

必须证实这个乘法的定义是合理的, 即乘积不依赖于相应的类中代表的选取. 设 $a' = a + x, b' = b + y$, 其中 $x, y \in J$. 则

$$a'b' = ab + ay + xb' = ab + z,$$

其中 $z = ay + xb' \in J$, 这是因为 J 是双边理想. 因此, $a'b'$ 和元素 ab 在同一个陪集中, 而这就是说乘积的定义 (2) 是合理的. 为了简短起见, 我们命 $\overline{a} = a + J$, 这样,

$$\overline{a} \oplus \overline{b} = \overline{a+b}, \quad \overline{a} \odot \overline{b} = \overline{ab}.$$

特别, $\overline{0} = J, \overline{1} = 1 + J$ (如果 K 中有单位元 1). 还必须证实对于有运算 $\oplus, \odot$ 的集合 $\overline{K} = K/J = \{\overline{a} | a \in K\}$, 所有的环公理都被满足. 但这是相当明显的, 这是因为 $\overline{K}$ 中剩余类的运算归结为 K 中元素的运算. 比方说, 分配性可以这样来验证:

$$(\overline{a} \oplus \overline{b}) \odot \overline{c} = \overline{(a+b)c} = \overline{(ac+bc)} = \overline{ac} + \overline{bc} = \overline{a} \odot \overline{c} + \overline{b} \odot \overline{c}.$$

所有这些指出了映射

$$\pi : a \mapsto \overline{a}$$

是环满同态 $K \to \overline{K}$, 其核 $\operatorname{Ker} \pi = J$. 从商环 $Z_m = \mathbb{Z}/m\mathbb{Z}$ 及满同态 $\mathbb{Z} \to Z_m$ 这一特例我们转向考虑任意环的情形.

现在我们注意到, 环的所有同态像本质上被 K 对于相应的理想的商环所穷尽. 事实上, 若 $f: K \to K'$ 是同态且 $f(K)$ 是环 K 关于 f 的像, 则用 $f(K)(\subset K')$ 来代替 K' 时, 我们就得到满同态. 为了不使记号复杂化, 我们一开始就认为 f 是满同态, 即我们认为 $f(K) = K'$. 根据 [BA I] 第 1 章中所说的一般原理, f 在 K 上确定

了一个等价关系 O_f; 在该情形, O_f 由将 K 分成陪集 $a+\operatorname{Ker} f=C_a$ 这一划分给出. 映射 f 确定了元素 $a'\in K'$ 与类 C_a 之间的一个双射, 即 $f'(C_a)=a'$, 若 $a'=f(a)$. 这时

$$f'(C_a+C_b)=f'(C_{a+b})=f(a+b)=f(a)+f(b)=f'(C_a)+f'(C_b),$$
$$f'(C_a\cdot C_b)=f'(C_{ab})=f(ab)=f(a)\cdot f(b)=f'(C_a)\cdot f'(C_b).$$

因此双射 f' 是同构 (为了简单起见, K 中的加法及乘法运算, 剩余类环 $K/\operatorname{Ker} f$ 中的加法及乘法运算和 K' 中的加法及乘法运算的记法相同: $+$ 及 $\cdot$).

实质上我们证明了

定理 1 (同态基本定理) *环 K 的任意一个理想 J 在商集 K/J 上确定了 (借助于公式 (1), (2)) 环的结构, 并且 K/J 是环 K 的同态像, 其核是 J. 反之, 环 K 的每一个同态像 $K'=f(K)$ 和商环 $K/\operatorname{Ker} f$ 同构.*

注 公式 (2) 的右端一般说来并不和剩余类 $a+J$ 及 $b+J$ 在集合论意义上的乘积一致. 例如, 当 $K=\mathbb{Z}, J=8\mathbb{Z}$ 时, 整数 $24\in 16+8\mathbb{Z}$ 不属于 $(4+8\mathbb{Z})^2$, 这是因为 $(4+8s)(4+8t)=16u$.

我们知道, $Z_m=\mathbb{Z}/m\mathbb{Z}$ 是域当且仅当 $m=p$ 是素数. 环 $\mathbb{Z}$ 和域 P 上多项式环 $P[X]$ 很类似, 其原因就是它们都是欧几里得环.

2. 多项式的分裂域 常常有这样的事情, 那就是看一下熟知的例子就有可能对它有更好的理解并进一步作出合理的普遍化.

定理 2 *下面的断言成立:*

i) 域 P 上多项式环 $P[X]$ 的每一个理想 J 都是主理想, 即对某一个多项式 f, 有 $J=(f(X)):=f(X)P[X]$;

ii) 商环 $P[X]/(f(X))$ 是域当且仅当 f 在 P 上不可约.

证明 i) 在 J 中取一个次数最小的多项式 f. 若 g 是 J 中任意一个多项式, 则被 f 除所作的带余除法 (P 是域, 因此无需担心 $g(X)$ 的最高次项系数的可逆性) 给出等式 $g=qf+r, \deg r<\deg f$, 由此推出 $r\in J$, 这是因为 g,f,qf 都是这个理想的元素. 根据 f 的取法, 我们得到结论: $r=0$. 这就是说, $g(X)$ 被 $f(X)$ 整除, 从而 $J=(f(X))=f(X)P[X]$, 即 J 由被 $f(X)$ 整除的多项式组成.

ii) 若 $f(X)=a(X)b(X), 0<\deg a(X), \deg b(X)<\deg f(X)$, 则剩余类 $\overline{a(X)}$, $\overline{b(X)}\in P[X]/(f(X))$ 都不是 $\bar{0}$. 但是

$$\overline{a(X)b(X)}=\overline{f(X)}=\bar{0}.$$

这就是说, $P[X]/(f(X))$ 有非平凡的零因子, 从而它不可能是域.

另一方面, $P[X]/(f(X))$ 中任意一个剩余类的代表中可能出现一个多项式 $a(X)$, $\deg a(X) < \deg f(X)$. 如果 $a \neq 0$, 而 f 不可约, 则存在 $b, c \in P[X]$ 使 $ab+cf=1$. 在这种情形, $\overline{a}\overline{b}+\overline{c}\overline{f}=\overline{1}$, 即 $\overline{a}\overline{b}=\overline{1}$. 这就是说, 任意一个剩余类 $\overline{a} \neq \overline{0}$ 都是可逆的, 从而环 $P[X]/(f(X))$ 是域. □

我们着重指出, 元素 $\overline{a}=a+(f)$ (其中 $a \in P$) 在 $P[X]/(f)$ 中组成一个和域 P 同构的子环. 在不可约多项式 $f(X)$ 的情形, 根据定理 2, 商环 $P[X]/(f)$ 是域, 它包含一个和 P 同构的子域.

推论　对于域 P 上任意一个不可约多项式 $f(X)$, 存在扩张 $F \supset P$, 在其中 $f(X)$ 至少有一个根. F 可以取为与 $P[X]/(f)$ 同构的域.

证明　我们把注意力转向特殊的元素 $\overline{X} \in P[X]/(f)$. 对于任意的 $a_0, a_1, \cdots, a_m \in P$, 我们有

$$\begin{aligned}\sum_{k=0}^{m} \overline{a}_k \overline{X}^k &= \sum_k \{a_k+(f)\}\{X+(f)\}^k = \sum_k \{a_k+(f)\}\{X^k+(f)\} \\ &= \left\{\sum_k a_k X^k\right\}+(f) = \overline{\sum_k a_k X^k}.\end{aligned}$$

简言之, 若 $g(Y)=\sum\limits_k a_k Y^k \in P[Y]$, 则 $g(\overline{X})=\overline{g(X)}$. 当将 P 和与它同构且被包含在 $P[X]/(f)$ 中的域等同起来的时候, $g(\overline{X})$ 这种记法当然是有意义的. 特别,

$$f(\overline{X})=\overline{f(X)}=f+(f)=(f)=\overline{0},$$

即元素 $\overline{X} \in P[X]/(f)$ 是多项式 f 的一个根. □

注　根据定理 1, 我们有同构 $\mathbb{C}=\mathbb{R}[i] \cong \mathbb{R}[X]/J$, 其中 $J=\{f \in \mathbb{R}[X] \mid f(i)=0\}$. 因为当 $(a,b) \neq (0,0)$ 时, $a+ib \neq 0$, 且因 $i^2+1=0 \Longrightarrow X^2+1 \in J$, 所以从证明定理 2 时所作的推理可以推出 $J=(X^2+1)\mathbb{R}[X]$. 商环 $\mathbb{R}[X]/J$ 的元素是陪集 $(a+bX)+J; a,b \in \mathbb{R}$; 对应 $a+ib \mapsto (a+bX)+J$ 确立了 $\mathbb{C}$ 和 $\mathbb{R}[X]/J$ 之间的同构.

和已经建立起来的术语相适应, 习惯上说, 推论中的扩张 $F \supset P$ 是通过对 P 添加多项式 f 的一个根 c 得到的: $F=P(c)$. 这时 $f(X)=(X-c)g(X)$, 其中 $g \in F[X]$. 我们有了现实的可能去构造域 P 的一个扩张, 在其中多项式 f 完全分解成线性因式的乘积.

定义　设 P 是域, f 是 $P[X]$ 中一个 n 次标准多项式, 它不一定是不可约的. 若在 $F[X]$ 中 $f(X)=(X-c_1)\cdots(X-c_n)$, 且 $F=P(c_1,\cdots,c_n)$, 即 F 是由对 P 添加多项式 f 的根 $c_1,\cdots,c_n$ 得到的, 则扩张 $F \supset P$ 叫做 f 在 P 上的**分裂域**.

定理 3　对于每一个次数为 $n>0$ 的标准多项式 $f \in P[X]$, 至少存在一个分裂域.

证明 标准这一条件无关紧要, 使用它只是为了方便. 设

$$f(X)=f_1(X)\cdots f_r(X)$$

是 f 在 $P[X]$ 中分解成不可约的标准因式的分解式. 根据定理 2 的推论, 存在扩张 $P_1\supset P$, 在其中多项式 f_1 至少有一个根. 这个根 c_1 当然也是 f 的一个根.

设已求得扩张 $P_k\supset\cdots\supset P_1\supset P$, f 在其上有分解式

$$f(X)=(X-c_1)\cdots(X-c_k)g_1(X)\cdots g_s(X),$$

它有 k 个 (不一定是不相同的) 线性因式, $k<n$. 再一次将定理 2 的推论应用于域 P_k 和不可约的标准多项式 $g_1\in P_k[X]$, 我们构造域 $P_{k+1}\supset P_k$, 在其中可以分出多项式 $g_1(X)$的, 从而也是多项式 $f(X)$ 的一个线性因式 $X-c_{k+1}$, 其中 $c_{k+1}\in P_{k+1}$. 如此继续下去, 我们得到在某个扩张 $P_n\supset P$ 上 f 完全分解成线性因式的乘积. 或者是 P_n, 或者是它的一个子域 F 就将是 f 的分裂域. 不排除 F 可能和 P 相同. □

为了可以谈论多项式的分裂域的唯一性, 定理 3 的证明中含有过多的随意想象. 虽然事实上多项式的分裂域精确到同构是唯一确定的, 但我们要到下一章中才来证明. 现在我们仅限于考察分裂域的一些例子.

1) 二次域 $\mathbb{Q}(\sqrt{d})$ 是多项式 X^2-d 的分裂域.

2) 如果对 Z_2 添加不可约多项式 X^2+X+1 的一个根 θ, 则得到由四个元素组成的域 $Z_2(\theta)=\{0,1,\theta,1+\theta\}$, 它和域 $Z_2[X]/(X^2+X+1)$ 同构, 也和 [BA I] 第 4 章 §3 第 5 目中的域 GF(4) 同构. 我们注意到

$$X^2+X+1=(X-\theta)(X-\theta^2),$$

即 $Z_2(\theta)$ 是多项式 X^2+X+1 的分裂域.

3) 多项式 X^2+1 不仅仅是在 $\mathbb{R}$ 上不可约的. 如果将 X^2+1 认作是 $\mathbb{R}$ 上不可约多项式, 则 $\mathbb{C}$ 就是它的分裂域. 但它也是在其它域上不可约的. 比如, 它在 Z_3 上是不可约的. 设 $\theta^2=-1$ (如果方便的话, 设 $\theta=X+(X^2+1)Z_3[X]$, 它是剩余类域 $Z_3[X]/(X^2+1)$ 的元素). 因为 $X^2+1=(X-\theta)(X-\theta^3)$, 所以 $Z_3(\theta)=\{a+b\theta|a,b\in Z_3\}$ 是 X^2+1 在 Z_3 上的分裂域.

顺便说一说, $Z_3(\theta)$ 和 [BA I] 第 4 章 §3 习题 11 中由矩阵 $\begin{pmatrix} a & b\\ -b & a\end{pmatrix}$ $(a,b\in Z_3)$ 所组成的域同构. 这里相应的映射是

$$a+b\theta\mapsto a\begin{pmatrix}1&0\\0&1\end{pmatrix}+b\begin{pmatrix}0&1\\-1&0\end{pmatrix}$$

我们把注意力转向

$$\begin{aligned}&Z_3(\theta)^*=\langle\lambda\rangle,\quad \lambda=1+\theta,\quad \lambda^2=-\theta,\quad \lambda^3=1-\theta,\\ &\quad\lambda^4=-1,\quad \lambda^5=-1-\theta,\quad \lambda^6=\theta,\quad \lambda^7=-1+\theta,\quad \lambda^8=1,\end{aligned}$$

即域 $Z_3(\theta)$ 的乘法群不仅是交换群, 而且是循环群, 这是预先就定了的.

4) 根据艾森斯坦 (Eisenstein) 的判别法, 多项式 X^3-2 在 $\mathbb{Q}$ 上是不可约的. 因为它的根并不都是实的, 所以 $\mathbb{Q}(\sqrt[3]{2})$ 不可能是分裂域. 事实上 $\mathbb{Q}(\sqrt[3]{2},\varepsilon)$ 是 X^3-2 的分裂域, 其中 ε 是 1 的一个 3 次本原根:

$$X^3-2=(X-\sqrt[3]{2})(X-\varepsilon\sqrt[3]{2})(X-\varepsilon^2\sqrt[3]{2}).$$

至于说到若干个独立变量的多项式的环, 则在 $\mathbb{R}[X,Y]$ 中已明显, 并非所有理想都是主理想.

例 由满足 $h(0,0)=0$ 的多项式组成的集合

$$J=\{Xf+Yg|f,g\in\mathbb{R}[X,Y]\}$$

明显是 $\mathbb{R}[X,Y]$ 的理想. 因为 $1\in\mathbb{R}[X,Y]$, 所以由 $J=q(X,Y)\mathbb{R}[X,Y]$ 将推出 $q(X,Y)\in J$. 因此 $q(0,0)=0$, 从而 $\deg q\geqslant 1$. 我们有 $X,Y\in J$, 于是

$$X=qu,\quad Y=qv.$$

由此必定推出等式 $\deg u=\deg v=0$, 即 $u,v\in\mathbb{R}$, 于是 $Y=u^{-1}vX$, 矛盾. 这一矛盾表明理想 J 不是主理想.

3. 环的同构定理 我们已经掌握了相当多的各种类型的环, 并且也掌握了从给出的环构造新环的方法. 构造矩阵环 $M_n(K)$, 分式域 $Q(K)$ 和多项式环 $K[X_1,\cdots,X_n]$ 就是例子, 其中 K 是交换环 (在 $Q(K)$ 的情形是整环). 在第 1 章中对群已经确立了关于同态的一些一般性事实, 我们还要来探讨环的与之相类似的一般性事实, 虽然只是简略地探讨一下, 但这是有好处的. 一般说来, 它的证明与群的情形没有什么不同, 留给读者作为习题.

对于环的同态基本定理 (定理 1), 我们补充两个同构定理.

定理 4 设 K 是环, L 是子环, J 是 K 的理想. 则 $L+J=\{x+y|x\in L,y\in J\}$ 是 K 的子环, 且含 J 作为理想, $L\cap J$ 是 L 的理想. 映射

$$\varphi: x+J\mapsto x+(L\cap J),\quad x\in L$$

是环的同构:

$$(L+J)/J\cong L/(L\cap J).$$

证明 头两个结论完全是明显的. 至于说最后一个结论, 则需要考虑自然满同态 $\pi:K\to K/J$ 的限制 $\pi_0=\pi|_L$. 它的像 $\mathrm{Im}\pi_0$ 由陪集 $x+J(x\in L)$ 组成, 即 $\mathrm{Im}\pi_0=(L+J)/J$. 满同态 $\pi_0: L\to(L+J)/J$ 的核 $\mathrm{Ker}\pi_0$ 由使得 $x+J=J$ 的元素 $x\in L$ 组成. 这就是说, $\mathrm{Ker}\pi_0=L\cap J$. 根据定理 1, 对应 $\overline{\pi}_0: x+(L\cap J)\mapsto\pi_0(x)=x+J$ 确立了同构 $L/(L\cap J)\cong(L+J)/J$. 剩下的只要再注意到 $\varphi=\overline{\pi}_0^{-1}$. □

我们进行与第 1 章 §4 中定理 3 的证明相仿的探讨以强调指出这与群论是完全平行的.

定理 5 设 K 是环, J, L 是 K 的子环且 J 是 K 的理想, 并且 $J \subset L$. 则 $\overline{L} = L/J$ 是 K/J 的子环, 而且 $\pi^*: L \to L$ 是 K 中包含 J 的子环的集合 $\Omega(K, J)$ 到环 $\overline{K}$ 的所有子环的集合 $\Omega(\overline{K})$ 上的一个双射. 若 $L \in \Omega(K, L)$, 则 L 是 K 的理想当且仅当 $\overline{L}$ 是 $\overline{K}$ 的理想, 并且

$$K/L \cong \overline{K}/\overline{L} = (K/J)/(L \cap J).$$

其证明是一个容易的习题 (见第 1 章 §4 中定理 4 的证明).

推论 设 K 是有单位元 1 的交换环 · 理想 J 在 K 中是极大的当且仅当商环 K/J 是域.

在环 K 的理想的集合中, 定义以下运算:

和 $J_1 + J_2 = \{x_1 + x_2 | x_k \in J_k\}$;

交 $J_1 \cap J_2 = \{x | x \in J_1, x \in J_2\}$;

积 $J_1 J_2 = \left\{\sum_i x_{1i} x_{2i} | x_{ki} \in J_k\right\} \subset J_1 \cap J_2$.

也可以谈论任意有限多个理想的和、交及积, 并且以下结论成立.

命题 若在有单位元的环 K 中, 对于理想 $J, J_1, \cdots, J_n$, 等式

$$J + J_k = K, \quad k = 1, \cdots, n$$

成立, 则等式

$$J + J_1 \cap J_2 \cap \cdots \cap J_n = K = J + J_1 J_2 \cdots J_n$$

也成立.

证明 因为 $J_1 J_2 \cdots J_n \subset J_1 \cap J_2 \cap \cdots \cap J_n$, 所以只需确立等式 $J + J_1 J_2 \cdots J_n = K$ 就够了. $n = 1$ 时, 根据条件, 结论是成立的. 当 $n = 2$ 时, 我们有

$$1 = 1^2 = (x_1 + y_1)(x_2 + y_2) = x + y_1 y_2,$$

其中 $x_1, x_2, x \in J, y_i \in J_i$. 这就是说, $1 \in J + J_1 J_2$, 从而 $K = J + J_1 J_2$. 接下去对于数 n 用归纳法就明显了. □

设 $K_1, K_2, \cdots, K_n$ 是有限多个环, $K = K_1 \times \cdots \times K_n$ 是集合的笛卡儿积. 对 K 引入环结构, 这里是按分量定义加法及乘法运算:

$$(x_1, \cdots, x_n) + (y_1, \cdots, y_n) = (x_1 + y_1, \cdots, x_n + y_n);$$

$$(x_1, \cdots, x_n) \cdot (y_1, \cdots, y_n) = (x_1 y_1, \cdots, x_n y_n).$$

我们得到环 K_i 的外直和 $K = K_1 \oplus \cdots \oplus K_n$. 在满同态 $\pi_i : (x_1, \cdots, x_n) \mapsto x_i, 1 \leqslant i \leqslant n$ 下, 每一个分量 K_i 是像. 又若

$$J_i = \{(0, \cdots, x_i, \cdots, 0) | x_i \in K_i\},$$

则 $J_i \cong K_i, J_i$ 是 K 的理想且 $K = J_1 + \cdots + J_n$.

现在设 K 是有理想 $J_1, \cdots, J_n$ 的环, 且

$$K = J_1 + \cdots + J_n,\ J_k \cap \left(\sum_{j \neq k} J_j \right) = 0, \quad 1 \leqslant k \leqslant n,$$

则 $K = J_1 \oplus \cdots \oplus J_n$ 是它的**理想 J_k 的内直和**. 就像在群论中一样, 环的内外直和之间的区别纯粹是集合论意义上的, 将它们用符号区别开没有意义.

习 题

1. 证明: 由所有有理数 a/b (其中 b 不被一个固定素数 p 整除) 组成的环 $Q_M(\mathbb{Z})$ 含有唯一的极大理想 $J = \{a/b \in Q_M(\mathbb{Z}) | p$ 整除 $a\}$. 每一个有唯一极大理想的环叫*局部环*.
2. 证明: 在任意一个有极大理想 $\mathfrak{M}$ 的局部环 K 中, 不属于 $\mathfrak{M}$ 的元素是可逆的.
3. 有单位元的环 K 的一个理想 $\mathcal{P}$ 叫做**素理想**, 如果商环 $K/\mathcal{P}$ 是整环. 每一个极大理想都是素理想. 在环 K 中的补 $M = K \backslash \mathcal{P}$ 是乘法子集 (不含 0 的幺半群). 在这些条件下, 环 $Q_M(K)$ 常用记号 $M^{-1}K$ 来记或者简单地记作 $K_{\mathcal{P}}$.

   证明: 环 $K_{\mathcal{P}}$ 恒是局部环, 且其极大理想 $\mathfrak{M}_{\mathcal{P}}$ 由形如 a/b 的商组成, 其中 $a \in \mathcal{P}, b \in K \backslash \mathcal{P}$. 并证明: $\mathfrak{M}_{\mathcal{P}} \cap K = \mathcal{P}$.

   从 K 转向局部环 $K_{\mathcal{P}}$ 的操作叫做环 K 关于素理想 $\mathcal{P}$ 的**局部化**.

§2 关于环的一些结果

本节可以看作是对 [BA I] 中第 4 章及第 5 章的不大的然而是有益的补充.

1. 高斯整数 以前证明过欧几里得环是唯一因子分解环. 属于这种环的有环 $\mathbb{Z}$ 和 $P[X]$. 下面我们还要举一个欧几里得环的例子, 而在后面则要举出是唯一因子分解环但不是欧几里得环的例子.

定理 1 *高斯整数环 $\mathbb{Z}[i]$ 是欧几里得环.*

证明 我们注意到, 数环

$$\mathbb{Z}[i] = \{m + in | m, n \in \mathbb{Z}\}$$

被包含在二次域 $\mathbb{Q}(i) \subset \mathbb{C}$ 中, 其中 $i^2+1=0$, 并且在几何上, 和复数平面 $\mathbb{C}$ 上整数格的结点的集合一致. 易知 $\mathbb{Z}[i]$ 是整环. 我们在 $\mathbb{Z}[i]^* = \mathbb{Z}[i]\backslash\{0\}$ 上定义一个映射 $\delta : \mathbb{Z}[i]^* \to \mathbb{N} \cup \{0\}$, 其中

$$\delta(m+in) = |m+in|^2 = m^2+n^2$$

(即 $\delta(a) = N(a)$ 是数 a 在 $\mathbb{Q}(i)$ 中的范数). 众所周知, 对所有的 $a, b \in \mathbb{Z}[i]^*, \delta(ab) = \delta(a)\delta(b)$, 因此欧几里得环的定义中的条件 E 1) (见 [BA I] 第 5 章 §3 第 3 目) 自动地被满足. 为了证明 E 2) 被满足, 我们将分数 ab^{-1} (其中 $b \neq 0$) 写成 $ab^{-1} = \alpha + i\beta$ (其中 $\alpha, \beta \in \mathbb{Q}$) 的形状, 并取最接近于 α, β 的整数 k, l 使 $\alpha = k+\nu, \beta = l+\mu, |\nu| \leqslant 1/2, |\mu| \leqslant 1/2$. 则

$$a = b[(k+\nu)+i(l+\mu)] = bq+r,$$

其中 $q = k+il \in \mathbb{Z}[i]$, 而 $r = b(\nu+i\mu)$. 因为 $r = a-bq$, 故也有 $r \in \mathbb{Z}[i]$, 并且

$$\delta(r) = |r|^2 = |b|^2(\nu^2+\mu^2) \leqslant \delta(b)\left(\frac{1}{4}+\frac{1}{4}\right) = \frac{1}{2}\delta(b) < \delta(b).$$

从而 $\mathbb{Z}[i]$ 是欧几里得环. □

将高斯整数环 $\mathbb{Z}[i]$ 作为模型一样来展示代数数论的方法, 这是合适的. 因此我们停下来对 $\mathbb{Z}[i]$ 的性质作稍为详细些的探讨. 首先我们来证明一些简单的断言.

定义 整环 K 叫**主理想环**, 若其所有理想都是主理想, 即其理想具有 aK 这种形状.

命题 1 所有欧几里得环都是主理想环.

证明 对于 $\mathbb{Z}$ 和 $P[X]$ 这早就被证明过 ([BA I] 及由 §1 定理 2), 而在一般情形, 它的推理是完全类似的: 若 J 是欧几里得环 K 的一个理想, 则只要 $a \in J$ 且 $\delta(a) \leqslant \delta(x)$ 对所有 $0 \neq x \in J$, 就有 $J = aK$. □

命题 2 设 K 是带有函数 δ 的任一欧几里得环, 且 $U(K)$ 是其可逆元组成的群, 则

$$u \in U(K) \Longleftrightarrow \delta(u) = \delta(1) \Longleftrightarrow \delta(ux) = \delta(x) \quad \forall x \in K^* \tag{1}$$

证明 事实上, 根据 E 1), 对所有 $x \in K^*$ 我们有 $\delta(x) = \delta(1 \cdot x) \geqslant \delta(1)$, 而如果 $u \in U(K)$, 则 $\delta(1) = \delta(uu^{-1}) \geqslant \delta(u)$. 因此 $\delta(u) = \delta(1)$. 反之, 根据命题 1,

$$\delta(ux) = \delta(x), \quad \forall x \in K^* \Longrightarrow uxK = xK \Longrightarrow x = uxv \Longrightarrow uv = 1 \Longrightarrow u \in U(K). \ \square$$

当应用于环 $\mathbb{Z}[i]$ 时, 判别法 (1) 意味着 $m+in \in U(\mathbb{Z}[i]) \Longleftrightarrow m^2+n^2 = 1$, 于是 $U(\mathbb{Z}[i]) = \langle i \rangle$ 是 4 阶循环群.

定义 环 K 的理想 J 叫做**极大的**, 若 $J \neq K$ 且每一个真包含 J 的理想 T 与 K 一致.

命题 3 在欧几里得环 K 中, 元素 $p \in K$ 是素元这一性质和理想 pK 是极大理想这一条件等价.

证明 事实上, 设 p 是素元且 $pK \subset T \subset K$, 其中 T 是 K 的理想. 根据命题 1, $T = aK$, 又因为 $p \in T$, 所以 $p = ab$, 其中元素 a, b 中有一个是可逆元. 若 $b \in U(K)$, 则 $T = aK = abK = pK$.

反之, 设理想 pK 是极大的, 且 $p = ab$, 其中 $a \notin U(K)$. 则 $aK \neq K$ 且 $pK \subset aK \Longrightarrow pK = aK \Longrightarrow a = pu = abu \Longrightarrow bu = 1 \Longrightarrow b \in U(K) \Longrightarrow p$ 是素元. □

2. 两个平方之和的标准分解 现在我们来看一看, 对于素数 $p \in \mathbb{Z}$, 在环 $\mathbb{Z}[i]$ 中会发生什么事情. 不排除 p 在 $\mathbb{Z}[i]$ 仍是素元. 在相反的情形, 有下面的

命题 4 若素数 $p \in \mathbb{Z}$ 在 $\mathbb{Z}[i]$ 中有非平凡分解, 则

$$p = (m + in)(m - in) = m^2 + n^2 \tag{2}$$

其中 $m + in, m - in$ 是 $\mathbb{Z}[i]$ 中素元.

证明 设 $p = \prod\limits_{k=1}^{r} p_k$ 是它分解成素元 p_k 的积的唯一分解式, 且 $r > 1$ (根据 [BA I] 第 5 章 §3 中的定理 4). 根据命题 2 有 $\delta(p_k) > 1$. 因此由 $p^2 = \delta(p) = \prod \delta(p_k)$ 及 $\mathbb{Z}$ 的唯一因子分解性, 必定有等式

$$r = 2, \quad p = p_1 p_2, \quad \delta(p_1) = \delta(p_2) = p.$$

若 $p_1 = m + in$, 则

$$p = \delta(p_1) = m^2 + n^2 = (m + in)(m - in) \Longrightarrow p_2 = m - in.$$ □

特别地, $2 = (1 + i)(1 - i)$ 在 $\mathbb{Z}[i]$ 中不是素元.

现在我们已准备好去证明下面的判别法.

定理 2 素数 $p \in \mathbb{Z}$ 在 $\mathbb{Z}[i]$ 中仍是素元当且仅当 $p = 4k - 1$.

每一个素数 $p = 4k + 1$ 可表示成 $p = m^2 + n^2$ 的形状, 其中 $m, n \in \mathbb{Z}$.

证明 首先我们注意到对于任何 $t \in \mathbb{Z}$ 有 $t^2 \equiv 0 (\operatorname{mod} 4)$ 或 $t^2 \equiv 1 (\operatorname{mod} 4)$. 因此对于在 $\mathbb{Z}[i]$ 中不是素元的奇素数 p, 命题 4 导致结论

$$p = m^2 + n^2 \equiv 0, 1, 2 (\operatorname{mod} 4) \Longrightarrow p = 4k + 1.$$

在 $p = 4k + 1$ 的情形, 命 $t = (2k)!$. 因为明显有

$$\begin{aligned} t = (-1)^{2k}(2k)! &= (-1)(-2)\cdots(-2k) \equiv (p-1)(p-2)\cdots(p-2k) \\ &\equiv ((p+1)/2)\cdots(p-2)(p-1) \quad (\operatorname{mod} p), \end{aligned}$$

所以

$$t^2 \equiv (2k)!((p+1)/2)\cdots(p-2)(p-1) \equiv (p-1)! \pmod p,$$

或者, 注意到威尔逊 (Wilson) 定理 ([BA I] 第 6 章 §1), $t^2+1 \equiv 0 \pmod p$. 现在假定 p 是 $\mathbb{Z}[i]$ 中素元, 则由等式 $(t+i)(t-i) = t^2+1 = lp, l \in \mathbb{Z}$, 根据 [BA I] 第 5 章 §3 中的定理 1, 推得元素 $t+i, t-i$ 中有一个被 p 整除. 但 $t \pm i = p(m+n) \Longrightarrow \pm 1 = pn, n \in \mathbb{Z}$, 这明显是不可能的. □

从已被我们确立的事实可以并不复杂地推导出一般的数论定理.

定理 3 数 $t \in \mathbb{Z}$ 可被表示成两个数 $m, n \in \mathbb{Z}$ 的平方之和当且仅当在 t 分解成素因子之积的标准分解式中出现的每一个素因子 $p = 4k-1$ 的指数是偶数.

证明 事实上只要证明, 若 $\text{g.c.d}(m,n) = 1$ 且 $p|(m^2+n^2)$, 则 $p = 4k+1$. 这是相当明显的, 如果我们注意到

$$\text{g.c.d}(m,n) = 1, \quad m^2+n^2 \equiv 0 \pmod p, \quad mn \not\equiv 0 \pmod p \Longrightarrow m^{p-1} \equiv 1 \pmod p,$$
$$n^2 \equiv -m^2 \pmod p \Longrightarrow (m^{p-2}n)^2 = m^{2p-4}n^2 \equiv -m^{2p-2} \equiv -1 \pmod p.$$

因此, 存在整数 $s \in \mathbb{Z}$ 使得 $s^2 \equiv -1 \pmod p, s^4 \equiv 1 \pmod p$. 于是乘法群 $\mathbb{Z}^*$ 的阶 $p-1$ 被 4 整除, 从而 $p = 4k+1$. □

根据命题 3, $p = 4k-1$ 在 $\mathbb{Z}[i]$ 是素元等价于理想 $p\mathbb{Z}[i]$ 是极大理想, 也就是商环 $\mathbb{Z}[i]/p\mathbb{Z}[i]$ 是 p^2 个元素组成的域 (关于这一点, 见 [BA I] 第 4 章 §3 习题 11 及 §1 中环的同构定理). 如果考虑到 $p = 4k-1$ 时 Z_p 上的多项式 X^2+1 是不可约的, 这也是不足为奇的. 关于这个问题将在下一章中更详细地谈一谈.

3. 唯一因子分解环的多项式扩张 我们指出, 多项式环 $\mathbb{Z}[X_1, \cdots, X_n]$ 及 $P[X_1, \cdots, X_n]$ (P 是域) 对于任何 P 都是唯一因子分解环. 这个重要的结论可直接由下面的定理推出.

定理 4 若环 K 是唯一因子分解环, 则多项式环 $K[X]$ 也是唯一因子分解环.

证明 作为证明基础的是多项式的一些性质. 这些性质与本原性概念及高斯引理有关 ([BA I] 第 5 章 §3). 即我们需要下面两个性质.

a) 若本原多项式 $f, g \in K[X]$ 在 $Q(K)[X]$ ($Q(K)$ 是唯一因子分解环 K 的分式域) 中是相伴的, 则它们在 $K[X]$ 中也是相伴的 (容易的习题).

b) 若次数为正数的多项式 $f \in K[X]$ 在 K 上是不可约的, 则它在 $Q(K)$ 上也是不可约的 ([BA I] 中对于 $K = \mathbb{Z}$ 的证明适用于一般情形).

在着手对定理进行证明时, 我们将次数为正数的多项式 $f \in K[X]$ 改写成 $f = d(f)f_0$ 的形状, 其中 $d(f)$ 是多项式 f 的容度, 而 f_0 是它的本原部分. 对本原多项式

的次数用归纳法, 我们得到 f_0 分解成 K 上不可约本原多项式 $f_1, \cdots, f_s$ 的积的分解式 $f_0 = f_1 \cdots f_s$.

若 $f_0 = g_1 \cdots g_t$ 又是一个这样的分解式, 则根据 b), f_i 及 g_i 在 $Q(K)$ 上不可约, 而因为环 $Q(K)[X]$ 是唯一因子分解环 (见 [BA I] 第 5 章 §3 定理 4 的推论), $s = t$, 并且在适当的排序下, f_i 和 g_i 在 $Q(K)[X]$ 中是相伴的, 从而 (根据 a)) 在 $K[X]$ 中也是相伴的.

至于说到多项式 f 在 K 中的容度 $d(f)$ 不可逆的情形, 则再取分解式 $d(f) = p_1 \cdots p_r$, 其中 $p_i \in K$ 是素元, 我们又得到 f 的一个分解式. 这种分解式的唯一性 (在通常意义下) 从刚刚确立的 f_0 的分解唯一性及由 $d(f) = p_1 \cdots p_r$ 的唯一性的 K 的因子分解唯一性所保证推出. □

定理 5 *存在严格的包含:*

$$\{\text{欧几里得环}\} \subset \{\text{主理想环}\} \subset \{\text{唯一因子分解环}\}. \tag{3}$$

证明 第一个包含由命题 1 推出. 存在着例子 (我们不举出它们) 表明它是严格的包含关系.

为了证明第二个包含, 我们考察主理想环 K 的理想的递增序列 $(d_1) \subset (d_2) \subset \cdots$. 可以直接检验出 $D = \bigcup_i (d_i)$ 是 K 的理想. 因此 $D = (d)$. 根据定义, 对某个 m, 有 $d \in (d_m) \subset D$, 由此得到 $(d_m) = (d_{m+1}) = \cdots$. 递增的理想链在有限步后的稳定引起不可逆因子链 $d_1, d_2, d_3, \cdots$ (其中 $d_i | d_{i+1}$) 的断裂, 因此在 K 中存在分解成不可分解元素的因子分解式.

K 中因子分解式的唯一性是以下事实的推论:

$$(a, b) = aK + bK = dK = (d) \Longrightarrow d = \mathrm{g.c.d}(a, b) = ax + by.$$

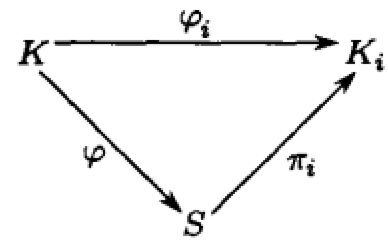
进一步的推理只是重复 [BA I] 第 5 章 §3 中定理 3 的推论 (ii) 的证明.

$\mathbb{Z}[X]$ 中的理想 $(2, X)$ 及 $\mathbb{R}[X, Y]$ 中的理想 (X, Y) 不是主理想 (见 §1 中的例子). 同时, 根据定理 4, 环 $\mathbb{Z}[i]$ 及 $\mathbb{R}[X, Y]$ 是唯一因子分解环. 因此, 链 (3) 的真实性被确立. □

主理想环从纯代数观点来看是有意思的, 这是因为它们的特性是由如同同态的核那样一些自然的对象的性质刻画出来的. 另一方面, 欧几里得环由于在其中存在带余除法的算法而对于研究更为方便.

4. 乘法群 $\mathrm{U}(Z_n)$ 的结构 直和的泛性质包含在以下相当明显的结论中.

设 $S = K_1 \oplus \cdots \oplus K_n$ 且 K 是任意环, 并已给同态 $\varphi_i : K \to K_i$, 则存在唯一的同态 $\varphi = (\varphi_1, \cdots, \varphi_n : K \to S)$, 其核是 $\mathrm{Ker}\,\varphi = \cap \mathrm{Ker}\varphi_i$, 使下列三角形图是交换的, $i = 1, \cdots, n$ (π_i 是自然映射).



我们将这一结论应用于有单位元 1 和理想 $J_1, \cdots, J_n$ 的环及直和

$$S = K/J_1 \oplus \cdots \oplus K/J_n.$$

命 $\varphi_i : K \to K/J_i = K_i$, 我们得到环 K 到 S 的同态

$$\varphi : x \mapsto (x + J_1, \cdots, x + J_n), \tag{4}$$

其核 $\mathrm{Ker}\varphi = J_1 \cap \cdots \cap J_n$.

定理 6 (中国剩余定理) *若在上面所指出的条件下, K 是含单位元的环, 且 $J_i + J_j = K$ 对 $1 \leqslant i \neq j \leqslant n$, 则映射 φ (见 (4)) 是满同态.*

证明 我们需要证明, 对任何给定的元素 $x_1, \cdots, x_n \in K$, 存在 $x \in K$ 使 $x_i + J_i = x + J_i$, 即 $x - x_i \in J_i, i = 1, 2, \cdots, n$. 当 $n = 1$ 时, 这是明显的, 而当 $n = 2$ 时, 取元素 $a_1 \in J_1, a_2 \in J_2$ 使 $a_1 + a_2 = 1$, 并命 $x = x_1 a_2 + x_2 a_1$, 则

$$x - x_1 = (x_1 a_2 + x_2 a_1) - x_1(a_1 + a_2) = (x_2 - x_1)a_1 \in J_1,$$
$$x - x_2 = (x_1 a_2 + x_2 a_1) - x_2(a_1 + a_2) = (x_1 - x_2)a_2 \in J_2.$$

然后对 n 用归纳法进行推理. 假设我们已经找出元素 y 使 $y - x_i \in J_i, i = 1, 2, \cdots, n-1$. 因为根据条件, $J_i + J_n = K, 1 \leqslant i \leqslant n-1$, 所以根据 §1 中的命题有 $J_1 \cap \cdots \cap J_{n-1} + J_n = K$. 将我们对于 $n = 2$ 已得到的结果应用于理想 $J_1 \cap \cdots \cap J_{n-1}, J_n$ 及元素 $x - x_n \in J_n$. 但是

$$x - y \in J_1 \cap \cdots \cap J_{n-1} \Longrightarrow x - y \in J_i, \quad 1 \leqslant i \leqslant n-1,$$

考虑到 y 的取法, 我们得到

$$x - x_i = (x - y) + (y - x_i) \in J_i, \quad 1 \leqslant i \leqslant n-1.$$

因此, 元素 x 满足所提出的全部要求. □

在定理 6 中及其论证前, 并不假定环 K 是交换环. 进一步设 K 是整环且 $a_1, \cdots, a_n$ 是它的 n 个两两互素的元素, 即 $a_i K + a_j K = K$ 对 $i \neq j$ (在唯一分解整环 K 中, 这个定义和将 a_i 分解成素因子之积所得到的互素的定义一致). 将包含关系 $x - x_i \in aK$ 写成模主理想 $a_i K$ 的同余式的形状, 我们像通常一样, 使用记号 $x \equiv x_i (\operatorname{mod} a_i)$.

推论 1 设 K 是整环且 $a_1, \cdots, a_n$ 是它的两两互素的元素, 则对任何 $x_1, \cdots, x_n \in K$, 存在元素 $x \in K$ 使

$$x \equiv x_i \pmod{a_i}, \quad i = 1, \cdots, n.$$

推论 2 设 n 是自然数, 其标准分解式是 $n = p_1^{m_1} \cdots p_r^{m_r}$, $Z_n = \mathbb{Z}/n\mathbb{Z}$ 是模 n 的剩余类环, 且 $U(Z_n)$ 是其可逆元组成的乘法群, 则

i) $Z_n \cong Z_{p_1^{m_1}} \oplus \cdots \oplus Z_{p_r^{m_r}}$ (环的直和);

ii) $U(Z_n) \cong U(Z_{p_1^{m_1}}) \times \cdots \times U(Z_{p_r^{m_r}})$ (群的直积).

证明 i) 用 r 代替 (4) 中的 n, 并命

$$K = \mathbb{Z}, \quad J_i = p_i^{m_i}\mathbb{Z}, \quad S = Z_{p_1^{m_1}} \oplus \cdots \oplus Z_{p_r^{m_r}},$$

我们得到同态 $\varphi : \mathbb{Z} \to S$, 其核 $\mathrm{Ker}\varphi = \bigcap\limits_i J_i = n\mathbb{Z}$. 因为 $i \neq j$ 时 $\mathrm{g.c.d}(p_i, p_j) = 1$, 所以由定理 6 推得 φ 是满射.

ii) 因为在任意直和 $K = K_1 \oplus \cdots \oplus K_r$ 中, 诸分量 K_i 互相零化: $K_iK_j = 0, i \neq j$. 所以由可逆元的定义直接推出 $U(K) = U(K_1) \times \cdots \times U(K_r)$. 剩下的只要将这一点应用分解式 i). □

注 由结论 (ii) 直接明显地看出 $\varphi(n) = \prod\limits_{i=1}^{r} \varphi(p_i^{m_i})$, 而因为 $\varphi(p^m) = p^{m-1}(p-1)$, 所以重又得到欧拉函数值公式 (见 [BA I] 第 1 章 §9 习题 3). 有限群的元素的阶是群的阶的因子, 因此对于和 n 互素的任意数 a, 有

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

(费马小定理的推广, 以欧拉定理之名闻名).

为了完全地了解群 $U(Z_n)$ 的结构, 根据定理 6 的推论 2, 我们只需考察 $n = p^m$ 的情形.

定理 7 设 m 是正整数.

i) 若 p 是奇素数, 则 $U(Z_{p^m})$ 是循环群.

ii) 群 $U(Z_2)$ 和 $U(Z_4)$ 是阶分别为 1 和 2 的循环群, 这时 $U(Z_{2^m}) (m \geqslant 3)$ 是阶为 2^{m-2} 的循环群和阶为 2 的循环群的直积.

证明 i) 根据定义, 如果 $|\langle t + n\mathbb{Z} \rangle| = r$, 则和 n 互素的整数 t 模 n 的阶是 r, 即 $t^r \equiv 1 \pmod{n}$, 但 $k < r$ 时 $t^k \not\equiv 1 \pmod{n}$. 当 $r = \varphi(n)$ 时, 则称 t 是**模 n 的本原根** (**或原根**). 通常 t 是模 n 的剩余系 $0, 1, \cdots, n-1$ 中的一个, 但是我们并不固定任何一个剩余系.

根据第 2 章 §3 中的定理 11, 群 $Z_p^* = U(Z_p)$ 是循环群, 即存在模 p 的本原根 a_0. 因为 $a_0^{p^{m-1}} \equiv a_0 (\operatorname{mod} p)$, 所以整数 $a = a_0^{p^{m-1}}$ 也是模 p 的本原根. 另一方面

$$a^{p-1} = a_0^{p^{m-1}(p-1)} = a_0^{\varphi(p^m)} \equiv 1 (\operatorname{mod} p^m).$$

这就是说, 陪集 $\overline{a} = a + p^m\mathbb{Z}$ 在 $U(Z_{p^m})$ 中生成一个阶为 $p-1$ 的循环子群.

进一步,

$$(1+p)^p = \sum_{i=0}^{p} \binom{p}{i} p^i = 1 + p^2 + \frac{1}{2}(p-1)p^3 + \sum_{i \geqslant 3} \binom{p}{i} p^i.$$

因为 $p > 2$, 所以 $(1+p)^p \equiv 1 + p^2 (\operatorname{mod} p^3)$. 作归纳假定 $(1+p)^{p^j} \equiv 1 + p^{j+1} (\operatorname{mod} p^{j+2})$, 我们得到

$$\begin{aligned}(1+p)^{p^{j+1}} &= [1 + (1+sp)p^{j+1}]^p = \sum_{i=0}^{p} \binom{p}{i} (1+sp)^i p^{(j+1)i} \\ &= 1 + (1+sp)p^{j+2} + \frac{1}{2}(p-1)(1+sp)^2 p^{2(j+1)+1} + \cdots,\end{aligned}$$

由此

$$(1+p)^{j+1} \equiv 1 + p^{j+2} (\operatorname{mod} p^{j+3}),$$

特别, 有

$$(1+p)^{p^{m-1}} \equiv 1 (\operatorname{mod} p^m).$$

但是

$$(1+p)^{p^{m-2}} \equiv 1 + p^{m-1} \not\equiv 1 (\operatorname{mod} p^m),$$

因此代表为 $b = 1 + p$ 的陪集 $\overline{b} = 1 + p + p^m\mathbb{Z}$ 在 $U(\mathbb{Z}_{p^m})$ 中生成一个阶为 p^{m-1} 的循环群. 根据第 2 章 §3 中的命题 2, 阶 $p-1, p^{m-1}$ 互素的元素 $\overline{a}, \overline{b}$ 生成一个循环群 $\langle \overline{a}\overline{b} \rangle$, 其阶为

$$p^{m-1}(p-1) = \varphi(p^m) = |U(Z_{p^m})|.$$

对于群 $U(Z_2)$ 及 $U(Z_4)$ 来说, 一切都是清楚的. 当 $m > 2$ 时, 从平凡的同余式 $5 \equiv 1 + 2^2 (\operatorname{mod} 2^3)$ 出发, 对 j 用归纳法容易验证

$$5^{2^j} \equiv 1 + 2^{j+2} (\operatorname{mod} 2^{j+3}).$$

特别,

$$5^{2^{m-3}} \equiv 1 + 2^{m-1} \not\equiv 1 (\operatorname{mod} 2^m), \quad 5^{2^{m-2}} \equiv 1 (\operatorname{mod} 2^m),$$

于是 5 模 2^m 的阶是 2^{m-2}, 且陪集 $5 + 2^m\mathbb{Z}$ 在 $U(Z_{2^m})$ 中生成指数为 2 的循环子群. 我们注意到 $-1 + 2^m\mathbb{Z} \notin \langle 5 + 2^m\mathbb{Z} \rangle$, 这是因为

$$5^j \equiv -1 (\operatorname{mod} 2^m) \Longrightarrow 5^j \equiv -1 (\operatorname{mod} 4) \Longrightarrow 1 \equiv -1 (\operatorname{mod} 4),$$

矛盾. 因为 $|\langle -1+2^m\mathbb{Z}\rangle| = 2$, 所以

$$U(\mathbb{Z}/2^m\mathbb{Z}) = \langle 5+2^m\mathbb{Z}\rangle \times \langle -1+2^m\mathbb{Z}\rangle$$

是 $(2^{m-2},2)$ 型交换 2–群 (见第 2 章 §3). □

推论 *群 $U(Z_n)$是循环群 (或者等价地, 模 n 的本原根存在) 当且仅当整数 $n>1$ 具有形状 $2, 4, p^m$ 或 $2p^m$, 其中 p 是奇素数.*

习 题

1. 证明: 唯一因子分解环 K 的非零元 p 是素元当且仅当 K/pK 是整环.

2. 证明: 若整环 K 不是域, 则 $K[X]$ 不是主理想环.

3. 证明: 元素 $x+y\sqrt{-3}$ (其中 $x,y\in\mathbb{Z}$, 或者 $x=(2k+1)/2, y=(2l+1)/2, k,l\in\mathbb{Z}$) 组成整环 K. 验证它是有函数 $\delta = N$ ($\mathbb{Q}(\sqrt{-3})$ 中的范数) 的欧几里得环. 证明子环 $\mathbb{Z}(\sqrt{-3})\subset K$ 甚至不是唯一因子分解环.

4. 求高斯整数环的所有素元.

5. 在 K 是唯一因子分解环的情形, 改进定理 6 的推论以达到: 当 $a_1,\cdots,a_n$ 是两两互素的元素时, 引入元素 $\widetilde{a}_i = \prod\limits_{j\neq i} a_j$, 求出元素 $b_i\in K$ 使

$$b_i \equiv 1(\operatorname{mod} a_i),\quad b_i\equiv 0(\operatorname{mod}\widetilde{a}_i),\quad 1\leqslant i\leqslant n.$$

设 $x_1,\cdots,x_n\in K$. 引入元素 $x=\sum b_ix_i$, 并验证 $x\equiv x_i(\operatorname{mod} a_i), 1\leqslant i\leqslant n$ (在 $x_1,\cdots,x_n$ 的个数 n 较大的情形明显是方便的).

6. 将上面的习题应用于模 $a_1=5, a_2=9$ 及数偶 $(x_1,x_2)=(2,5),(3,2),(3,5)$. 关于 x 模 45 的阶能说些什么?

7. 设 p 是奇素数. 若同余式 $x^2\equiv a(\operatorname{mod} p)$ 有解, 则整数 a 叫做模 p 的**二次剩余**, 在相反的情形, 叫做**二次非剩余**. 勒让德 (Legendre) 符号 $\left(\dfrac{a}{p}\right)$ 由关系式

$$\left(\frac{a}{p}\right)=\begin{cases}0, & 若 a\equiv 0(\operatorname{mod} p),\\ 1, & 若 a\not\equiv 0(\operatorname{mod} p), a\ 为二次剩余,\\ -1, & 若 a\not\equiv 0(\operatorname{mod} p), a\ 为二次非剩余\end{cases}$$

定义. 证明: $\left(\dfrac{a}{p}\right)=1 \iff a+p\mathbb{Z}\in (Z_p^*)^2$ 且 $\left(\dfrac{a}{p}\right)\equiv a^{\frac{p-1}{2}}(\operatorname{mod} p)$. 进而, $\left(\dfrac{ab}{p}\right) = \left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$ 且在给出的 $1,2,\cdots,p-1$ 中, 二次剩余的个数和二次非剩余的个数相等. 对于不大的奇素数 p 及 q, 验证曾被高斯用多种方法对一般情形证明了的高斯互逆定理

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

由定理 1 导出关系式 $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

8. 证明 (用前面习题中的符号): $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, 即 2 是 $\bmod p$ 的平方当且仅当 $p \equiv \pm 1 (\bmod 8)$.

9. (对 [BA I] 第 3 章 §4 的补充). 设 $f(X) = f(\cdots, x_{ij}, \cdots)$ 是 n^2 个独立变量 $x_{ij} \in K, 1 \leqslant i, j \leqslant n$, 其系数在 $\mathbb{Z}$ 中或在某个域中的非零多项式, 并将其视作矩阵 $X = (x_{ij})$ 的函数. 证明: 若 $f(XY) = f(X)f(Y)$ 对所有 $X, Y \in M_n(K)$, 则 $f(X) = (\det X)^m$, 其中 m 是某个非负整数. 特别, 若 $f(\operatorname{diag}(x, 1, \cdots, 1)) = x$, 则 $f(X) = \det X$.

§3 模

模的概念是近百年来在代数学中所创造出的基本原理的载体. 其原因在于任何代数系统的研究不应仅是研究这一系统的内部性质, 而且也应研究它的全部表示 (在这个词的最广泛的意义下).

1. 关于模的初步知识 我们从经典的定义开始. 设 K 是有单位元的结合环, V 是用加法记出的交换群. 又设给出了从 $K \times V$ 到 V 的映射 $(x, v) \mapsto xv$, 它满足条件:

M1) $x(u+v) = xu + xv$,

M2) $(x+y)v = xv + yv$,

M3) $(xy)v = x(yv)$,

M4) $1 \cdot v = v$

对所有 $x, y \in K, u, v \in V$. 则 V 叫做**左 K–模** (或**环 K 上左模**). 类似地定义右 K–模. 以后我们简单地说 K–模, 虽然在某些场合两种模一起出现.

如果环 K 没有单位元的话, 公理 M4) (酉模条件) 自然是多余的. 更为本质的可以修改公理 M3), 使适合于一些非结合环. 非结合环上模的例子将在本章末举出. 暂时我们将从上面给出的定义出发.

设 V 是 K–模, $U \subset V$ 是子群. 如果对所有 $x \in K, u \in U, xu \in U$, 则子群 U 叫做 V 的**子模**.

进一步, 设 U 和 V 是任意 K–模, U 到 V 的映射 $\sigma : U \to V$ 若对所有 $u_1, u_2, u \in U, x \in K$ 满足

$$\sigma(u_1 + u_2) = \sigma(u_1) + \sigma(u_2),$$
$$\sigma(xu) = x\sigma(u),$$

则 σ 叫做 **K–模同态** (或简称 **K–同态**). 容易验证, $\operatorname{Ker}\sigma = \{u \in U | \sigma(u) = 0\}$ 是 U 的 K–子模, 而像 $\operatorname{Im}\sigma$ 是 V 的 K–子模.

对于每一个 K 上子模 $U \subset V$, 有**商模** $V/U = \{v + U | v \in V\}$ (交换群的加法商群), 其按照规则

$$x(v + U) = xv + U$$

定义 K 对它的运算. 我们对群证明了的, 然后又对环证明了的同态基本定理和两个同构定理可以逐字逐句地转到模上, 只要对其中的证明作不重要的改变.

在第 1 章后, 考察了 M3), M4) 型的公理, 在切切实实地论述了群表示 (公理 M1), M3), M4)) 的第 3 章之后, 我们举出了 K–模的例子, 它未必给人以新鲜的感觉. 然而值得对它们进行探讨并作互相对比.

1) 每一个交换群 A 是 $\mathbb{Z}$–模. 即从 $\mathbb{Z}\times A$ 到 A 的映射 $(n,a)\mapsto na$ 满足全部公理 M1)—M4). 将交换群当作 $\mathbb{Z}$ 上模的观点是非常有益的. 我们在第 2 章中描述有限生成交换群时证实了这一点. 在那里, 事情的本质就是使用了全部的模的术语.

2) 每一个交换群 A 是它自己的**自同态环** $\mathrm{End}\,A$ 上的模. 根据定义, $\mathrm{End}\,A$ 由所有满足条件 $\varphi(a+a')=\varphi(a)+\varphi(a')$ 的映射 $\varphi:A\to A$ 组成. $\mathrm{End}\,A$ 中的加法及乘法运算按自然方式引入:

$$(\varphi+\psi)(a)=\varphi(a)+\psi(a),\quad (\varphi\psi)(a)=\varphi(\psi(a)),\quad 1(x)=x, 0(x)=0.$$

显然, 从 $\mathrm{End}\,A\times A$ 到 A 的映射 $(\varphi,a)\mapsto\varphi(a)$ 给予了 A 以 $\mathrm{End}\,A$–模的结构.

3) 域 P 上向量空间 V 无疑是 P–模. 如果还给出了线性变换 $\mathcal{A}:V\to V$, 并且对于任意 $v\in V$ 及任意多项式 $f\in P[X]$, 命

$$f(X)v=f(\mathcal{A})v=a_0v+a_1\mathcal{A}v+\cdots+a_k\mathcal{A}^kv$$

则就给予了 V 以多项式环 $P[X]$ 上模的结构, 记作 $V_{\mathcal{A}}$. 公理 M1)—M4) 被满足, 这是因为连同 $\mathcal{A}$ 一起, 变换 $f(\mathcal{A})$ 也将是线性的, 并且

$$(f+g)(\mathcal{A})=f(\mathcal{A})+g(\mathcal{A}),\quad fg(\mathcal{A})=f(\mathcal{A})g(\mathcal{A})$$

(多项式环的通有性质). $V_{\mathcal{A}}$ 的子模是 $\mathcal{A}$–不变子空间. 同一个空间 V 的不同线性变换一般说对应着不同的 (不同构的) $P[X]$–模.

4) 环 K 的任意左理想 J 被给予自然的 K–模结构, 其运算是 $(x,y)\mapsto xy, x\in K, y\in J$, 它由 K 中的乘法运算导出. 在 $J=K$ 的情形, 环 K 看作是它自身上的模 ${}_KK$, 对 K 的这种观点导致有成效的结果.

5) 回到前面的例子, 我们构造商模 $K/J=\{y+J|y\in K\}$. 根据一般的定义, $(x,y+J)\mapsto xy+J$ 是 K 对 K/J 的运算. 我们看到, 自然满同态 $\pi:K\to K/J$ 是 K–模同态, 它满足关系 $\pi(xy)=xy+J=x(y+J)=x\pi(y)$. 而如果 J 是双边理想, 则 K/J 是环且 π 是环同态: $\pi(xy)=\pi(x)\pi(y)$.

任意多个 K 上子模 $V_i\subset V$ 的交 $\bigcap\limits_i V_i$ 是 V 的子模. 特别地, 包含给定集合 $T\subset V$ 的所有子模的交导致**子模** $\langle T\rangle$, **它由集合** T **生成**且由所有可能的形如 $x_1t_1+\cdots+x_st_s$ 的元素组成, 其中 $x_i\in K, t_i\in T$. 顺便说说, 我们注意到非零元素 $t_1,\cdots,t_s\in V$ 叫做在 K 上**线性相关**, 若 $x_1t_1+\cdots+x_st_s=0$, 其中并非所有 x_i

都等于零. 一组子模 $\{V_1,\cdots,V_m\}$ 生成的子模叫做这些子模的**和**并按通常方式记作 $\sum\limits_i V_i = V_1+\cdots+V_m$.

由单独一个元素 $v\in V$ 生成的 K 上的模 V 叫做**循环模**, 它具有形状 $V=Kv=\{xv|x\in K\}$ 它是循环群的类似物. 特别地, 循环模 $_KK=K\cdot 1$ (见例 4) 是群 $(\mathbb{Z},+)$ 的类似物.

若 $V=Kv_1+\cdots+Kv_n$ 是有限多个循环模的和, 则模 V 叫做**有限生成模**或**有限型模**.

容易验证, 映射 $x\mapsto xv$ 是模同态 $_KK\to Kv$. 它的核 $\mathrm{Ann}(v)=\mathrm{Ann}_K(v)=\{x\in K|xv=0\}$ 是 K 的左理想, 叫做元素 v 的**零化子** (或**挠率**). 因此, $Kv\cong K/\mathrm{Ann}(v)$. 使 $\mathrm{Ann}(v)\neq 0$ 的元素 $v\in V$ 叫做**周期的**. 所有元素都是周期元的模也叫做**周期的**. 若 V 不含非零的周期元, 则称 V 是**无挠模**.

集合

$$\mathrm{Ann}(V)=\{a\in K|aV=0\}=\bigcap_{v\in V}\mathrm{Ann}(v)$$

叫做 K–模 V 的**零化子** (或**挠率**). 若 $\mathrm{Ann}(V)=0$, 模就叫做**忠实模**.

可以从另外的方面来得到这一概念. 设 $V(x)$ 是 V 中被元素 $x\in K$ 零化的元素 v 的集合. 若 K 是整环, 则 $V(x)+V(y)\subset V(xy)$ 且**挠子模**

$$\mathrm{Tor}(V)=\sum_{x\in K}V(x)$$

的概念有意义 (挠率来自 torsion (英语)). 在有等式 $\mathrm{Tor}(V)=V$ 的情形, 称 V 是**挠模**. 而如果 $\mathrm{Tor}(V)=0$, 则我们从新回到无挠模的概念.

周期模的具有代表性的例子: a) 每一个有限交换群 ($\mathbb{Z}$ 上有限型周期模; 挠率是 $m\mathbb{Z}$ 或群的素指数 m); b) 伴随着线性变换 $\mathcal{A}$ 的 $P[X]$ 上模 $V_{\mathcal{A}}$ (见例 3; 挠率是由线性变换 $\mathcal{A}$ 的极小多项式生成的主理想).

命题 1 *$\mathrm{Ann}(V)$ 恒是环 K 的双边理想. 命 $(x+\mathrm{Ann}(V))v=xv$, 我们就给予了 V 以忠实 $K/\mathrm{Ann}(V)$–模的结构.*

证明 命 $A=\mathrm{Ann}(V)$. 很清楚, A 是 K 中加法子群. 又, 对任意 $x,x'\in K, a\in A, v\in V$, 我们有 $(xax')v=xa(x'v)=(xa)v'=x(av')=x\cdot 0=0$, 由此推出 $KAK\subseteq A$, 即 A 是 K 的双边理想. 现在若 $x+A=x'+A$, 则 $x-x'\in A$, 由此得到 $(x-x')v=0$ 或 $xv=x'v$. 于是 $(x+A)v=(x'+A)v$, 即商环对 V 的运算的定义是正确的. 不难验证, 关于这一运算, V 是 (K/A)–模. 最后,

$$(x+A)V=0\Longrightarrow x+A\in\mathrm{Ann}_{K/A}(V)\Longrightarrow xV=0\Longrightarrow x\in A.$$

因此, K/A 中只有零元素零化 V. □

由命题 1 推出, 商环 $K/\mathrm{Ann}(V)$ 和环 $\mathrm{End}\,V$ 的一个子环同构 (见例 2).

若 V, W 是两个 K–模, 则所有 K–线性同态 $\sigma : V \to W$ 所组成的集合 $\mathrm{Hom}_K(V, W)$ 关于同态的逐点相加的运算

$$\begin{aligned}(\sigma+\tau)(xv) &= \sigma(xv)+\tau(xv) = x\sigma(v)+x\tau(v)\\ &= x(\sigma(v)+\tau(v)) = x((\sigma+\tau)(v))\end{aligned}$$

是交换群. 对于交换环 K 上的模 V, W, 集合 $\mathrm{Hom}_K(V, W)$ 本身是 K–模, 如果将 $x\sigma(x \in K, \sigma \in \mathrm{Hom}_K(V, W))$ 理解为映射 $v \mapsto x(\sigma(v))$ 的话:

$$\begin{aligned}(x\sigma)(yv) &= x\cdot\sigma(yv) = x(y\sigma(v)) = xy(\sigma(v))\\ &= (yx)(\sigma(v)) = y(x\sigma(v)) = y((x\sigma)(v)).\end{aligned}$$

在 $W = V$ 的情形, 集合 $\mathrm{End}_K(V) = \mathrm{Hom}_K(V, V)$ 是环; 乘法是 K–同态的自然合成 $\varphi\circ\psi$:

$$(\varphi\circ\psi)(xv) = \varphi(\psi(xv)) = \varphi(x\psi(v)) = x\varphi(\psi(v)) = x((\varphi\circ\psi)(v)).$$

应该记住, 当将 V 看作加法交换群时, 我们写成 $\mathrm{End}_{\mathbb{Z}}(V)$, 并且一般说来, $\mathrm{End}_K(V)$ 是 $\mathrm{End}_{\mathbb{Z}}(V)$ 的真子环. 在域 K 上向量空间 V 的情形, 通常我们写成 $\mathfrak{L}(V) = \mathrm{End}_K(V)$, 并称 $\mathfrak{L}(V)$ 是**线性变换环** (或线性变换**代数**).

模 V 的 K–自同态环 $\mathrm{End}_K(V)$ 还叫做**环 K 在 V 上的中心化子**. 它的作用在不可约模的情形特别显著. 环 K 上的模 V 叫做**不可约的** (或**单的**), 如果: a) $V \neq 0$; b) $0, V$ 是 V 的仅有子模; c) $KV \neq 0$ (若 K 含单位元, 则这个条件自动被满足). 很显然, K–模 $V \neq 0$ 是不可约模当且仅当 $V = Kv$ 是循环模, 对 V 中任何 $v \neq 0$.

命题 2 (舒尔 (Schur) 引理) 若 V, W 是两个不可约 K–模, σ 是 V 到 W 的非零 K–同态, 则 σ 是同构. 于是, 对于任意不可约 K–模 V, $\mathrm{End}_K(V)$ 是除环 (体).

证明 在第 3 章 §4 中也有一个舒尔引理 (定理 1), 在那里是对不可约 G–空间证明的.

2. 自由模 我们称 K–模 V 是其子模 $V_1, \cdots, V_n$ 的 **(内) 直和**, 若

$$V = V_1 + \cdots + V_n \quad 且 \quad V_i \cap \sum_{j\neq i} V_j = 0 \quad 对 \quad i = 1, \cdots, n.$$

换句话说, $V = V_1 \oplus \cdots \oplus V_n$ (子模直和的记号), 若任意元素 $v \in V$ 可唯一地写成线性组合 $v = v_1 + \cdots + v_n (v_i \in V_i)$ 的形状. K–模 $V_1, \cdots, V_n$ **的外直和**以明显的方式定义 (和环的情形一样), 其元素 $x \in K$ 对行 $(v_1, \cdots, v_n)$ 的运算是 $x(v_1, \cdots, v_n) = (xv_1, \cdots, xv_n)$.

进一步, 设 V 是 K–模, $\{v_1,\cdots,v_n\}$ 是 V 的一个有限子集. 称 $\{v_1,\cdots,v_n\}$ 自由地生成 V, 若 $V=Kv_1+\cdots+Kv_n$ 且集合 $\{v_1,\cdots,v_n\}$ 到任意一个 K–模 W 的每一个映射 φ 都可以延伸为一个 K–同态 $\widetilde{\varphi}:V\to W$ 使 $\widetilde{\varphi}(v_i)=\varphi(v_i), 1\leqslant i\leqslant n$.

由某个子集 $\{v_1,\cdots,v_n\}$ 自由地生成的 K 上的模 V 叫做**秩为 n 的自由模**, 而 $\{v_1,\cdots,v_n\}$ 叫做它在 K 上的 **(自由) 基**.

命题 3 以下断言等价:

i) 集合 $\{v_1,\cdots,v_n\}$ 自由地生成 V;

ii) 集合 $\{v_1,\cdots,v_n\}$ 线性无关且 $\langle v_1,\cdots,v_n\rangle=V$;

iii) 每一个元素 $v\in V$ 可唯一地写成 $v=\sum_i x_iv_i$ 的形状, 其中 $x_i\in K$;

iv) $V=Kv_1\oplus\cdots\oplus Kv_n$ 是直和且 $\mathrm{Ann}(v_i)=0$;

v) $V\cong {}_KK\oplus\cdots\oplus {}_KK$ 是 ${}_KK$ 的 n 个拷贝的直和 (因此, 基为 $\{v_1,\cdots,v_n\}$ 的秩为 n 的自由 K–模同构于长度为 n 的分量 $x_i\in K$ 的行 $(x_1,\cdots,x_n)$ 组成的模 K^n).

证明 和 [BA II] 中对域上线性空间所进行的论证相近, 但是对于牵涉到环 K 的非交换性或 K 中非可逆元的存在性等处需小心谨慎. □

有相当复杂的非交换环的例子: 当 $m\neq n$ 时, 非交换环 K 有 $K^m\cong K^n$. 然而对于交换环则不会发生这种情况.

命题 4 整环上有限生成模的秩唯一确定.

证明 设 $\{v_1,\cdots,v_n\},\{u_1,\cdots,u_m\}$ 是 K 上自由模 V 的两个基. 则

$$v_j=\sum_{i=1}^m a_{ij}u_i,\quad u_i=\sum_{k=1}^n b_{ki}v_k.$$

由于 K 的交换性, 对于 $m\times n$ 矩阵 $A=(a_{ij})$ 及 $n\times m$ 矩阵 $B=(b_{ki})$, 有关系式

$$AB=E_m,\quad BA=E_n.$$

将 K 嵌入分式域 $Q(K)$, 借助于 [BA I] 第 2 章 §3 中的定理 3 (不仅对于 $\mathbb{R}$ 成立, 而且对于任意域成立), 我们得到 $\min(n,m)\geqslant m, \min(n,m)\geqslant n$, 由此得到 $m=n$. 补充说一句, $m<\infty, n=\infty$ 这种情形是不可能的, 这是因为在 u_i 的表达式中, 只出现有限多个自由地生成整个模 V 的基元素 v_k. □

注 在含单位元的任意交换环 K 的情形, 若在 K 中取一个极大理想 J 并转向域 K/J, 则我们将达到和命题 4 同样的效果. 我们省略掉细节.

我们注意到, 和向量空间的情况不同, 任意取出的自由 K–模的生成集未必含有模的基. 例如, 两个不相同的素数 p,q 恒生成 ${}_\mathbb{Z}\mathbb{Z}$, 这是因为存在 $u,v\in\mathbb{Z}$ 使 $up+vq=1$. 但是由于 $p\cdot q-q\cdot p=0$. 所以 $\{p,q\}$ 不是基, 而 $\mathbb{Z}p,\mathbb{Z}q$ 是 ${}_\mathbb{Z}\mathbb{Z}$ 的真子模.

自由模的作用是在它的定义中已设计好了的.

定理 1 任意有限型 K–模是有限型自由 K–模的同态像.

证明 设 $U=\sum_{i=1}^{n}Ku_i$ 是由 n 个元素 $u_1,\cdots,u_n$ 生成的 K–模. 取具有基 $\{v_1,\cdots,v_n\}$ 的自由 K–模 V. 它的存在性是由命题 3 保证的. 根据自由模的定义, 映射 $\varphi:v_i\mapsto u_i$ 可以延伸为 K–同态 $\widetilde{\varphi}:V\to U$. 像 $\mathrm{Im}\,\widetilde{\varphi}$ 含有模 U 的生成集, 从而含有整个模 U. □

自由模的子模并非恒是自由的, 即使它是它的直加项. 这里有一个最简单的例子. 设 $K=Z_6, U=K(2+6\mathbb{Z}), W=K(3+6\mathbb{Z})$. 则 $K=U\oplus W$ 是 K–模 U,W 的直和, 它们当中没有一个是自由的: $|K|=6$, 这时 $|U|=3,|W|=2$.

定理 2 设 $V=Kv_1\oplus\cdots\oplus Kv_n$ 是主理想环 K 上秩为 n 的自由模. 则它的每一个子模 U 是秩为 $m\leqslant n$ 的自由模.

证明 首先设 $n=1$, 即 $V\cong K$. 任意子模 $U\subset V$ 和 K 的一个理想同构, 于是 $U\cong(u)=Ku$. 若 $u=0$, 则 $U=0$ (零子模可以认为是秩为零的自由模). 若 $u\neq 0$, 则对所有 $0\neq a\in K$ 有 $au\neq 0$, 这是因为 K 是整环. 这意味着 U 是秩为 1 的自由(循环) 模. 当 $n>1$ 时, 我们用归纳法进行论证.

在 V 中考察秩为 $n-1$ 的自由子模 $V'=Kv_2\oplus\cdots\oplus Kv_n$. 商模 $\overline{V}=V/V'$ 是自由模, 有循环生成元 $\overline{v}_1=v_1+V'$. 它有子模 $\overline{U}=(U+V')/V'$. 若 $\overline{U}=0$, 则 $U\subset V'$, 这时根据归纳假定, 定理的断言成立.

如果 $\overline{U}\neq 0$, 则上面对 $n=1$ 情形所进行的论证指出 $\overline{U}$ 有循环生成元 $\overline{u}_1=u_1+V'$, 其中 $u_1\in U$.

若 $U\cap V'=0$, 则

$$
\begin{aligned}
u\in U &\Longrightarrow \overline{u}=u+V'\in\overline{U}\Longrightarrow\overline{u}=a_1\overline{u}_1, a_1\in K\Longrightarrow u-a_1u_1\in V'\\
&\Longrightarrow u=a_1u_1\Longrightarrow U=Ku_1
\end{aligned}
$$

是秩为 1 的自由模.

最后, 设 $U\cap V'\neq 0$. 根据归纳假定, 秩为 $n-1$ 的自由模 V' 的子模 $U\cap V'$ 有自由基 $\{u_2,\cdots,u_m\}$, 其中 $0<m-1\leqslant n-1$. 几乎是逐字逐句地重复上面进行过的论证, 我们可以证实 $\{u_1,u_2,\cdots,u_m\}$ 是 U 的自由基. 事实上,

$$
\begin{aligned}
u\in U &\Longrightarrow \overline{u}=u+V'\in\overline{U}\Longrightarrow\overline{u}=a_1\overline{u}_1, a_1\in K\\
&\Longrightarrow u-a_1u_1\in U\cap V'\Longrightarrow u-a_1u_1=a_2u_2+\cdots+a_mu_m\\
&\Longrightarrow u=a_1u_1+a_2u_2+\cdots+a_mu_m,\quad m\leqslant n.
\end{aligned}
$$

根据命题 3, ii), 我们必须证实生成元 $u_1,\cdots,u_m$ 的线性无关性. 但是 $\sum_i x_iu_i=0\Longrightarrow$ 在 $\overline{V}$ 中有 $x_1\overline{u}_1=-\sum_{i>0}x_i\overline{u}_i=0$. 这就是说 $x_1=0$, 这是因为 $\overline{u}_1$ 是 $\overline{V}$ 的基而由于

$\{u_2, \cdots, u_m\}$ 是 $U \cap V'$ 的自由基, 所以

$$x_2u_2 + \cdots + x_mu_m = 0 \Longrightarrow x_2 = \cdots = x_m = 0. \qquad \square$$

推论· 主理想环上有限型模的每一个子模本身是有限型模.

其证明由定理 1, 2 及第二个同构定理 (关于子模之间的对应的定理) 得出.

要得到主理想环 K 上有限型模的完全描述一点也不复杂. 不过最有意思的情形我们已经考察过了 (第 2 章中和 [BA II] 第 2 章 §3 中的 $\mathbb{Z}$ 上及 $P[X]$ 上的周期模). 在处理其它问题中同样的模的方法的展示可以在补充文献中找到.

3. 环的整元素 设 K 是整环. 元素 $t \in K$ 叫做整的 (在 $\mathbb{Z}$ 上整的), 若 t 是标准多项式 $X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$ 的根. 在 K 是域 $\mathbb{Q}$ 的有限代数扩张或者 K 是所有复代数数生成的域的情形, 我们就说它们是代数整数, $\mathbb{Z}$ 的所有元素自然地归入它们. 容易看出 (也见第 5 章) 有理数 t 是代数整数当且仅当 $t \in \mathbb{Z}$. 进一步, 若 $a_0u^n + a_1u^{n-1} + \cdots + a_n = 0$, 则 $(a_0u)^n + a_0a_1(a_0u)^{n-1} + \cdots + a_0^na_n = 0$, 而这就是说, 任意代数数, 乘上一个适当的元素 $a_0 \in \mathbb{Z}$ 后, 就成为一个代数整数.

转向一般情形, 我们注意到, 将 K 当作 $\mathbb{Z}$–模是方便的. 任意元素 $t_1, t_2, \cdots, t_n \in K$ 在 K 中生成有限型子模 $Kt_1 + Kt_2 + \cdots + Kt_n$. 特别地, 若 t 是整元素且 $t^n + a_1t^{n-1} + \cdots + a_n = 0, a_i \in \mathbb{Z}$, 则子环 $\mathbb{Z}[t] \subset K$ 是有限型 $\mathbb{Z}$–模, 这是因为 $\mathbb{Z}[t] = \mathbb{Z}1 + \mathbb{Z}t + \cdots + \mathbb{Z}t^{n-1}$. 反之, 设 $\mathbb{Z}[t]$ 是有生成元 $v_1, \cdots, v_n \in K$ 的有限型 $\mathbb{Z}$-模, 则带有矩阵 $A = (a_{ij}) \in M_n(\mathbb{Z})$ 的关系式

$$tv_i = a_{i1}v_1 + a_{i2}v_2 + \cdots + a_{in}v_n, \quad 1 \leqslant i \leqslant n$$

导致一个结论: 看作分式域 $Q(K)$ 上的齐次线性方程组

$$\begin{aligned} &(t - a_{11})x_1 - a_{12}x_2 - \cdots - a_{1n}x_n = 0, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &-a_{n1}x_1 - a_{n2}x_2 - \cdots + (t - a_{nn})x_n = 0 \end{aligned}$$

有非零解 $(x_1, \cdots, x_n) = (v_1, \cdots, v_n)$ (不是所有 v_i 都等于零, 这是因为 $1 \in \mathbb{Z}[t]$). 这就是说, 方程组的行列式等于零 (见 [BA I] 第 3 章) 且 t 是标准多项式 $f(T) = \det(TE - A)$ 的根. 我们证明了, 元素 $t \in K$ 是整元素当且仅当子环 $\mathbb{Z}[t] \subset K$ 是有限型 $\mathbb{Z}$–模.

定理 3 环 K 的整元素在 K 中组成子环.

证明 设 $u, v \in K$ 是整元素. 则

$$\mathbb{Z}[u, v] = \sum_{i \leqslant n, j \leqslant m} \mathbb{Z}u^iv^j$$

是有限型 $\mathbb{Z}$–模. 因为 $\mathbb{Z}$ 是主理想环, 则定理 2 的推论 (或直接验证) 指出, 子模 $\mathbb{Z}[u-v], \mathbb{Z}[uv]$ 也是有限型 $\mathbb{Z}$–模. 根据上面得到的判别准则, 元素 $u-v, uv$ 应该是整元素. □

例 1 的任意次根 ε 显然是代数整数. 根据定理 3, 1 的根的整数线性组合也将是代数整数. 特别 (见第 3 章 §4 中命题的证明), 有限群 G 在 $\mathbb{C}$ 上的任意线性表示 Φ 的特征标 χ_Φ 的值 $\chi_\Phi(g)(g \in G)$ 是代数整数.

习 题

1. 利用 $\mathbb{C}[X]$ 上模的一般结果, 勾画出 JNF 定理 (见 [BA II]) 的证明提要.

2. 利用关于 $\mathbb{Z}$ 上模的一般性结果, 拟定一个关于有限生成交换群的定理的证明方案.

3. 设 $A = P[X_1, \cdots, X_n]$ 是域 P 上 n 个变量的多项式环. 由 r 个多项式 $f_i \in A$ 组成的序列 $(f_1, \cdots, f_r)$ 叫做是幺模的, 若 $Af_1 + Af_2 + \cdots + Af_r = A$, 即存在 $u_i \in A, 1 \leqslant i \leqslant r$ 使

$$u_1 f_1 + u_2 f_2 + \cdots + u_r f_r = 1 \tag{$*$}$$

进一步, 设 V 是 A 上有限型模. 鉴于代数几何学中一些微妙的问题, 法国数学家塞尔 (Serre,J.-P.) (1955 年) 提出了一个猜想

$$\{V \oplus A^s \cong A^{s+t} \Longrightarrow V \cong A^t\},$$

它被补充了下面精美的形式: 每一个关系式 $(*)$ 对于适当的 $u_{ij} \in A$ 可以写成等式

$$\begin{vmatrix} f_1 & f_2 & \cdots & f_r \\ u_{21} & u_{22} & \cdots & u_{2r} \\ \cdots & \cdots & \cdots & \cdots \\ u_{r1} & u_{r2} & \cdots & u_{rr} \end{vmatrix} = 1$$

的形状. 这一断言尽管表面上很简单, 但直到 1976 年才被苏斯林 (A.A.Суслин, 俄罗斯) 及奎林 (Д.Квиллен, 美国) 各自独立地证明. 试对不大的 n 及 r 证明它.

基本的思想是研究群 $\mathrm{GL}(r, A[X_1, \cdots, X_{n-1}])$ 在幺模序列集合上的作用并利用对 n 作归纳法. 关于证明可参阅原始论文: Суслин А. А.//ДАН СССР.—1976—Т.299, № 5.—1063~1066 页; 或 N. Bourbaki 讨论会上的报告: Ferrand D.//Sém. N. Bourbaki, 28ème annee, 1975/76, Juin 1976. 叙述完全是初等的. 它有多大价值可根据在 N. Bourbaki 讨论会上更早的报告: Bass H.//Sém. N. Bourbaki, 26ème annee, 1973/74, Juin 1974 来判断. 在所指出的文献中还提出了未解决的问题. 全部问题对于专业讨论会是非常好的.

§4 域上代数

1. 代数的定义及例子 我们已在不同场合用过代数的概念 (见第 1 章 §1 及 [BA I]、[BA II]), 所以在下面给出定义实际上只是为了叙述上的完整.

定义 域 P 上的**代数** (或**线性代数**) 由环 $(A,+,\cdot)$ 及 P 上向量空间 A 这一对组成 (环及向量空间的基础集合 A 是相同的; 加法运算 $+$ 及零元素 0 也是同样的). 并且对所有 $\lambda\in P, x,y\in A$, 有

$$\lambda(xy)=(\lambda x)y=x(\lambda y).$$

一个代数叫做**结合的**, 若环 $(A,+,\cdot)$ 是结合的. P 上向量空间的维数也叫做**代数 A 的维数**.

增加一些无关紧要的精确性就可将环论中的基本概念转移到代数上. 比如, 环 A 的每一个同时也是向量空间 A 的子空间的子环 B 就被认为是代数 A 的**子代数**. 如果 T 是 A 的子集, 则由它生成的子代数 $P[T]$ 是 A 中所有包含 T 的子代数的交. 以类似的方式定义理想及对于它们的商代数. 代数的同态是环的同态, 它同时也是 P–线性映射.

结合代数 A 的中心$Z(A)$ 定义为和 A 中每一个元素可交换的所有元素 $a\in A$ 组成的集合: $a\in Z(A)\Longleftrightarrow ax=xa, \forall x\in A$. 显然, 中心 $Z(A)$ 是 A 的子代数. 等式 $Z(A)=A$ 成立当且仅当 A 是交换代数.

若 A 是有单位元 1 的结合代数, 则直接验得 $\lambda\cdot 1\in Z(A)$, 并且对应 $\lambda\mapsto\lambda\cdot 1, \forall\lambda\in P$, 确定 P 到 A 的一个单射. 在这一意义下, 代数 A 可以理解成具有包含在中心 $Z(A)$ 中的子域的环 A.

我们举几个结合代数的例子.

1) 域 P 的有限 $[F:P]$ 次扩张 $F\supset P$ 显然是有限维 $(\dim_P F=[F:P])$ 交换结合代数 (有单位元).

2) 系数在域 P 中的多项式环 $K=P[X_1,\cdots,X_n]$ 带有域 P 上无限维交换结合代数的自然结构. 我们看到,

$$K=K_0\oplus K_1\oplus K_2\oplus\cdots$$

是 m 次齐次多项式组成的有限维向量子空间 $K_m(K_0=P)$ 的直和, 并且 $K_iK_j\subset K_{i+j}$. 这种类型的代数叫做**分次代数**.

3) 有限群 G 的所有特征标在 $\mathbb{C}$ 上生成的含单位元 χ_1 的交换代数 $X_{\mathbb{C}}(G)$ 的维数 r 等于 G 中共轭元素类的个数.

4) 系数在域 P 中的 n 阶方阵组成的环 $M_n(P)$ 是 P 上 n^2 维代数. 代数 $M_n(P)$ 的基元素 $\{E_{ij}|i,j=1,2,\cdots,n\}$ 按规则 $E_{ik}E_{lj}=\delta_{kl}E_{ij}$ 相乘. 根据 [BA I] 第 2 章 §3 中的定理 4, $Z(M_n(P))=\{\lambda E\}\cong P$.

称具有单位元的结合代数 A 在域 P 上是**中心单的**, 若 $Z(A)\cong P$ 并且 A 没有和 0 及 A 不相同的双边理想.

命题 1 $M_n(P)$ 是中心单代数.

证明 设 J 是 $M_n(P)$ 中和零理想不相同的理想, 并设

$$0 \neq a = \sum_{ij} a_{ij} E_{ij} \in J.$$

若 $a_{kl} \neq 0$, 则对任意 $s, t = 1, \cdots, n$, 有 $E_{st} = a_{kl}^{-1} E_{sk} \cdot a \cdot E_{lt} \in J$, 于是 $J = M_n(P)$.□

对于任意体 D 上的矩阵代数 $M_n(D)$, 类似的结论成立. 非常重要的韦德伯恩 (Wedderburn) 定理 (更一般的叫韦德伯恩–阿廷 (Artin) 定理) 说, *每一个域 P 上有限维结合代数同构于 $M_n(D)$, 其中自然数 n 唯一确定, 而体 D (是 P 上有限维代数) 精确到同构唯一确定.*

矩阵代数 $M_n(P)$ 还有以下泛性质.

命题 2 *每一个域 P 上 n 维结合代数同构于 $M_k(P)$ 的一个子代数, 其中 $k \leqslant n+1$.*

证明 首先我们将认为 A 是有 1 的代数, 并且我们将它嵌入 $M_n(P)$. 为此, 对于每一个元素 $a \in A$, 我们命它和向量空间 A 的一个线性变换 $L_a : x \mapsto ax$ 相对应. L_a 的线性性是 A 中乘法运算的双线性性的推论. 因为显然 $L_{\lambda a} = \lambda L_a, L_{a+b} = L_a + L_b, L_{ab} = L_a L_b$ (结合性) 且 $L_1 = \varepsilon$, 所以映射 $a \mapsto L_a$ 是同态. 它的单射性由单位元的存在所保证: $a \neq 0 \Longrightarrow L_a \cdot 1 = a \cdot 1 = a, L_a \neq 0$.

现在设 A 是没有单位元的代数. 我们考察向量空间 $\bar{A} = P \oplus A$ 并对它定义乘法

$$(\lambda, a)(\lambda', a') = (\lambda\lambda', aa' + \lambda a' + \lambda' a).$$

容易验证, 对于这种乘法, $\bar{A}$ 是域 P 上有单位元 $(1, 0)$ 的代数.

因为 $\dim_P \bar{A} = \dim_P A + 1 = n + 1$, 所以前面的论证允许将 $\bar{A}$, 同时也将 A 嵌入 $M_{n+1}(P)$. □

不难发现命题 2 的证明和关于有限群的凯莱定理的证明 ([BA I]) 是完全类似的. 在这两种情形都用了正则表示. 更一般地: P 上代数A 的表示理解为任意同态

$$A \to \mathfrak{L}(V) = \mathrm{End}_F(V),$$

其中 $F \supset P$ 是域 P 的某个扩张. 换句话说, F 上向量空间 V 被赋予了 §3 中定义意义下的左 A–模结构, 并且

$$(\lambda x) \cdot v = x \cdot (\lambda v) \quad \forall \lambda \in P, x \in A, v \in V.$$

在 V 中取定某个基, 像在群的情形一样, 我们得到矩阵表示 $A \to M_r(F)$, 其中 $r = \dim_F(V)$.

2. 可除代数 (体) 正如上面表述的韦德伯恩定理所指出的, 可除代数的研究是结合代数的一般结构理论的重要组成部分. 舒尔引理 (§3 中的命题 2) 也证实了这一想法. 在获得关于可除代数的一些结果以前, 我们先来证明一个辅助性断言.

命题 3 *在域 P 上 n 维结合代数 A (有单位元 1) 中, 每一个元素 $a \in A$ 是一个次数 $\leqslant n$ 的多项式 $\mu_a \in P[X]$ 的根. 元素 $a \in A$ 是可逆元当且仅当 $\mu_a(0) \neq 0$. 如果 A 没有零因子, 则 A 是可除代数. 若域 P 是代数闭的, 则 $n = 1, A = P$.*

证明 由于 A 是有限维的, 元素 $1, a, a^2, \cdots$ 不可能在 P 上全都是线性无关的. 于是存在最小次数为 $m \leqslant n$ 的标准多项式 $\mu_a(X) = X^m + \alpha_1 X^{m-1} + \cdots + \alpha_m$ (系数 $\alpha_i \in P$) 使得 $\mu_a(a) = 0$. 若 $\alpha_m \neq 0$, 则关系式 $\mu_a(a) = 0$ 被改写成

$$\left[-\alpha_m^{-1}\left(a^{m-1} + \alpha_1 a^{m-2} + \cdots + \alpha_{m-1}\right)\right] a = 1$$

的形状时, 它表明, a 是可逆元.

反之, 假定 $a \in A$ 不是零因子, 而 $\alpha_m = 0$. 则

$$\left(a^{m-1} + \alpha_1 a^{m-2} + \cdots + \alpha_{m-1}\right) a = 0 \Longrightarrow a^{m-1} + \alpha_1 a^{m-2} + \cdots + \alpha_{m-1} = 0,$$

它和 $\mu_a(X)$ 的极小性矛盾. 这意味着 $\alpha_m \neq 0$. 特别地, A 中所有不是零因子的元素都是可逆元.

若域 P 是代数闭的, 则

$$\mu_a(X) = (X - c_1) \cdots (X - c_m), \quad c_i \in P.$$

由此推得

$$(a - c_1)b = 0, \quad b = (a - c_2) \cdots (a - c_m) \neq 0$$

由于 A 中没有零因子, 所以只剩下唯一的一种可能性: $m = 1$ 及 $a - c_1 = 0, a = c_1 \in P$. 因为这对于任意元素 $a \in A$ 都是对的, 所以 $A = P$. □

我们看到, 可除代数的性质本质上依赖于基域 P. 在历史上, 实数域 $\mathbb{R}$ 上的可除代数自然地引起了人们特别的兴趣. 域 $\mathbb{C} = \mathbb{R} + i\mathbb{R}$ 的存在成为寻找其它"超复数系"的理由. 在第 1 章 §1 的第 5 目中考察了四元数代数 $\mathbb{H}$, 它是结合的但是是非交换的可除代数. 在涉及四元数的方面出现了下面的出色的定理, 且其证明也很巧妙.

定理 1 (弗罗贝尼乌斯 (Frobenius F. G.)) *在域 $\mathbb{R}$ 上只存在三个有限维结合的可除代数: $\mathbb{R}, \mathbb{C}$ 及 $\mathbb{H}$.*

在动手证明以前, 先对可除代数 A 的加法结构作些研究. 在下面的论证中, 我们从 [BA I, BA II] 知道的一种情况是非常重要的, 即任意元素 $0 \neq a \notin \mathbb{R}$ 的极小多项式 $\mu_a(t)$ (见命题 3) 应该是不可约的, 从而是二次的. 还注意到, $\mu_a(t)$ 不是别的,

它正好就是 A 的线性变换 $L_a: x \mapsto ax$ 的极小多项式. 更具体些, $\mu_x(t) = t - a$ 或 $t^2 - 2\alpha t + \beta, \alpha^2 < \beta$. 若 $x \notin \mathbb{R}$, 则命 $y = x - \alpha$, 就有 $\mu_y(t) = t^2 + (\beta - \alpha)^2$. 因此, A 中每一个元素具有 $\alpha + y$ 的形状, 其中 $\alpha \in \mathbb{R}, y = 0$ 或 $y^2 = \gamma < 0, \gamma \in \mathbb{R}$.

引理 1　子集

$$A' = \{u \in A | u^2 \in \mathbb{R}, u^2 \leqslant 0\}$$

是 A 的向量子空间.

证明　很清楚, $u \in A', \alpha \in \mathbb{R} \Longrightarrow \alpha u \in A'$, 因此, 只要证实, 对于不成比例的向量 u, v 有: $u, v \in A' \Longrightarrow u + v \in A'$.

首先我们验证不可能存在线性关系式 $u = \alpha v + \beta$ (其中 $\alpha, \beta \in \mathbb{R}$). 事实上, 根据条件, $uv \neq 0$ 且

$$u^2 = \gamma < 0, \quad v^2 = \delta < 0.$$

因此,

$$u = \alpha v + \beta \Longrightarrow \gamma = u^2 = (\alpha v + \beta)^2 = \alpha^2\delta + 2\alpha\beta v + \beta^2.$$

因为 $v \notin \mathbb{R}$, 所以 $\alpha\beta = 0$, 即 $\alpha = 0$ 或 $\beta = 0$. 若 $\alpha = 0$, 则 $u \in \mathbb{R}$, 而若 $\beta = 0$, 则 u 和 v 成比例. 这两种可能性已在前面被排除.

于是, $u, v \in A'$ 的线性无关性导致 $1, u, v$ 的线性无关性. 两个元素 $u + v, u - v$ 是二次方程的根, 即

$$(u+v)^2 = p(u+v) + q, \quad (u-v)^2 = r(u-v) + s, \quad p, q, r, s \in \mathbb{R}.$$

利用关系式

$$(u \pm v)^2 = u^2 \pm (uv + vu) + v^2, u^2 = \gamma, \quad v^2 = \delta,$$

将有

$$\gamma + \delta + (uv + vu) = p(u+v) + q,$$
$$\gamma + \delta - (uv + vu) = r(u-v) + s.$$

将它们相加, 得到

$$(p+r)u + (p-r)v + (q + s - 2\gamma - 2\delta) = 0.$$

然而如我们所看到的, $u, v, 1$ 是线性无关的, 因此 $p = r = 0$. 于是 $(u+v)^2 = q \in \mathbb{R}$, 而因为 $u + v \notin \mathbb{R}$, 所以 $q < 0$. 而这就是说, $u + v \in A'$, 即 A' 是 A 的子空间. □

定理 1 的证明　对于 $u \in A'$, 我们写 $u^2 = -q(u)$, 其中 $q(u) \in \mathbb{R}$ 且 $q(u) \geqslant 0$. 此外, $q(u) = 0 \Longleftrightarrow u = 0$. 显然 $q(\alpha u) = \alpha^2 q(u)$, 并且

$$f(u, v) := q(u+v) - q(u) - q(v) = -(uv + vu)$$

是对应于正定二次型 q 的 A 上的对称双线性型.

若 $A=\mathbb{R}$, 则论证完毕. 设 $A\neq\mathbb{R}$. 则 $A'\neq 0$, 并且我们可以选取向量 $\mathbf{i}\in A$ 使 $q(\mathbf{i})=1$, 即 $\mathbf{i}^2=-1$. 精确到同构, 我们得到等式 $\mathbb{R}[\mathbf{i}]=\mathbb{C}=\mathbb{R}+\mathbb{R}\mathbf{i}$. 若 $A=\mathbb{C}$, 则我们的论证又完毕.

我们认为 $A\not\supseteq\mathbb{C}$. 则 $A'\not\supseteq\mathbb{R}\mathbf{i}$, 并可选取元素 $\mathbf{j}\perp\mathbb{R}\mathbf{i}, q(\mathbf{j})=1$. 在这种情形, $\mathbf{j}^2=-1$ 且 $\mathbf{ij}+\mathbf{ji}=-f(\mathbf{i},\mathbf{j})=0$, 从而 $\mathbf{ij}=-\mathbf{ji}$. 命 $\mathbf{k}=\mathbf{ij}$, 我们得到 $\mathbf{k}^2=-1, \mathbf{ik}+\mathbf{ki}=0=\mathbf{jk}+\mathbf{kj}$. 因此 $\mathbf{k}\in A'$ 且 $\mathbf{k}\perp\mathbf{i},\mathbf{j}$. 于是 $1,\mathbf{i},\mathbf{j},\mathbf{k}$ 线性无关且

$$\mathbb{R}+\mathbb{R}\mathbf{i}+\mathbb{R}\mathbf{j}+\mathbb{R}\mathbf{k}=\mathbb{H}$$

是四元数代数.

若 $A\not\supseteq\mathbb{H}$, 则存在 $\mathbf{l}\in A'$ 使 $q(\mathbf{l})=1$ 且 $\mathbf{l}\perp\mathbf{i},\mathbf{j},\mathbf{k}$. 换句话说

$$\mathbf{li}=-\mathbf{il},\quad \mathbf{lj}=-\mathbf{jl},\quad \mathbf{lk}=-\mathbf{kl}.$$

然而由于 A 中乘法的结合性, 头两个关系式给出

$$\mathbf{lk}=\mathbf{l}(\mathbf{ij})=(\mathbf{li})\mathbf{j}=-(\mathbf{il})\mathbf{j}=-\mathbf{i}(\mathbf{lj})=\mathbf{i}(\mathbf{jl})=(\mathbf{ij})\mathbf{l}=\mathbf{kl}.$$

它和第三个关系式矛盾. 这就是说, $A=\mathbb{H}$. □

注 不太久以前, 在深刻的拓扑学考虑的基础上, 证明了 $\mathbb{R}$ 上每一个有限维可除代数 (不一定是结合的) 的维数是 1, 2, 4 或 8. 每一种可能性都得到了实现.

20 世纪初, 韦德伯恩 (Wedderburn) 得到了关于有限体的结果, 它对于几何学有重要意义. 现在我们来证明这个定理, 诚然, 是依据了下一章中确立的分圆多项式的一些初等性质. 但这里并不发生循环论证.

定理 2 (韦德伯恩) *每一个有限结合除环是交换的, 即它是域.*

证明 设 D 是有限除环, $Z=Z(D)$ 是它的中心. 显然 Z 是域且 D 是 Z 上有限维向量空间:

$$D=Ze_1\dotplus Ze_2\dotplus\cdots\dotplus Ze_n.$$

根据在第 5 章 §2 中确立的结果, 对某个 $q=p^m$, 有 $Z=\mathbb{F}_q$, 于是 $|D|=q^n$. 进一步, 设 $x\in D\backslash Z$. 与 x 可交换的元素组成集合 $C(x)=\{y\in D|yx=xy\}$, 它对加法及乘法运算是封闭的. 换句话说, $C(x)$ 是 D 中包含 Z 的可除子代数. 若 q^d 是 $C(x)$ 中元素的个数, 则 $d=d(x)$ 是 n 的因子, $d<n$, 这是因为将 D 解释成 $C(x)$ 上左向量空间

$$D=C(x)f_1\dotplus\cdots\dotplus C(x)f_r$$

时, 我们有 $q^n=|C(x)|^r=q^{dr}$. 现在注意到, Z^* 是乘法群 D^* 的中心, 而 $(q^n-1)/(q^d-1)=(D^*:C(x)^*)$ 是 D^* 中和 x 共轭的元素的个数, 因此第 1 章 §3 中的公

式 (2′) 有形状

$$q^n - 1 = |D^*| = (q-1) + \sum_d \frac{q^n - 1}{q^d - 1}, \tag{*}$$

其中 d 走遍 n 的小于 n 的因子的集合.

分圆多项式 $\Phi_n(X)$ 的性质 (见第 5 章 §2 的习题 6) 指出, 当 $d|n, d < n$ 时, 整数 $\Phi_n(q)$ 既整除 $q^n - 1$, 又整除 $(q^n - 1)/(q^d - 1)$, 而这导致 (见 §1 习题 7) 等式 $n = 1$, 从而导出 $D = Z$ 的交换性. □

3. 群代数及它上的模　和第 3 章 §1 中有限群 G 的正则表示相联系, 出现了域 K 上的向量空间 $\langle e_g | g \in G \rangle$. 现在命 $e_g e_h = e_{gh}$, 我们按线性性将这个规则推广到任意向量 $\sum \alpha_g e_g$ $(\alpha_g \in K)$ 上, 就将这个向量空间转变成 K–代数. 为了使记法简化, 通常用 g 来代替 e_g, 并考察所有可能的形式和 $\sum \alpha_g g$ $(\alpha_g \in K)$ 的集合 $K[G]$. 按定义

$$\sum_g \alpha_g g = \sum_g \beta_g g \Longleftrightarrow \alpha_g = \beta_g \quad \forall g \in G.$$

形式和的运算

$$\sum_g \alpha_g g + \sum_g \beta_g g = \sum_g (\alpha_g + \beta_g) g,$$

$$\lambda \left(\sum_g \alpha_g g \right) = \sum_g (\lambda \alpha_g) g, \tag{1}$$

$$\left(\sum_g \alpha_g g \right) \left(\sum_h \beta_h h \right) = \sum_{g,h} \alpha_g \beta_h gh = \sum_u \gamma_u u, \quad \gamma_u = \sum_g \alpha_g \beta_{g^{-1}u}$$

赋予 $K[G]$ 以结合代数的结构. 习惯上称 $K[G]$ 是**有限群 G 在域 K 上的群代数**. 空间 $K[G]$ 的基元素是等同于元素 $g \in G$ 的形式积 $1 \cdot g (g \in G)$; $\dim_K K[G] = |G|$. 因此, 群 G 被认为是嵌入 $K[G]$ 的. 单位元 $e \in G$ 是 $K[G]$ 的单位元. 当 K 是有单位元的交换结合环时, 得到群 G 在 K 上的**群环** $K[G]$.

此外, 如果限于只考虑仅有有限个不等于零的系数的和 $\sum \alpha_g g$, 类似的构造可被用于任意的未必是有限的群 G. 将 $S = \sum \alpha_g g$ 解释为群 G 上的函数是方便的: 函数值是 $S(g) = \alpha_g$ $(\alpha_g \in K)$ 且其值几乎处处是零, 即只有有限多个不为零的值. 这时公式 (1) 对应于逐点相加的运算

$$(S_1 + S_2)(g) = S_1(g) + S_2(g)$$

及函数的卷积

$$S_3 = S_1 * S_2, \quad S_3(u) = \sum_g S_1(g) S_2(g^{-1}u).$$

群环理论是代数学的一个内容丰富的分支, 它有自己的研究内容, 但对于我们来说, 这里 $K[G]$ 只不过是最后两章中引入的一般概念的实例.

定理 3 *在 $K[G]$–模 (它是域 K 上有限维向量空间) 和群 G 的线性表示之间存在相互单值的对应.*

证明 设 (Φ, V) 是群 G 的表示. 按线性性将 Φ 延伸到 $K[G]$ 的元素上. 定义

$$\widetilde{\Phi}\left(\sum \alpha_g g\right) = \sum \alpha_g \Phi(g),$$

并命

$$\left(\sum \alpha_g g\right) \circ v = \sum \alpha_g \Phi(g) v \quad \forall v \in V.$$

运算 "∘" 赋予 V 以 $K[G]$–模 (在这个词的通常意义下) 的结构.

我们看到

$$\begin{aligned}\left(\sum \alpha_g g\right) \circ (\lambda v) &= \sum \alpha_g \Phi(g)(\lambda v) = \sum \alpha_g \lambda \Phi(g) v \\ &= \lambda \left(\sum \alpha_g \Phi(g) v\right) = \lambda \left(\left(\sum \alpha_g g\right) \circ v\right),\end{aligned}$$

即用 V 中纯量来乘和用 $K[G]$ 中纯量来乘是一致的. 偶 $(\widetilde{\Phi}, V)$ 自然地叫做**代数 $K[G]$ 的线性表示**.

反之, 若 V 是 K 上向量空间, 并且又是 $K[G]$–模, 其运算是

$$\left(\sum \alpha_g g, v\right) \mapsto \left(\sum \alpha_g g\right) \circ v,$$

则命

$$\widetilde{\Phi}\left(\sum \alpha_g g\right) v = \left(\sum \alpha_g g\right) \circ v$$

时, 我们定义了一个同态 $\widetilde{\Phi} : K[G] \to \mathrm{End}_K(V)$ (即代数 $K[G]$ 的一个表示), 它在 G 上的限制 $\Phi = \widetilde{\Phi}|_G$ 给出了群 G 的一个表示. □

相应于定理 3, 群 G 的表示空间 V 常常叫做群 G 的**表示模**, 或简短地叫做 **G–模**. 相应的术语上的变更涉及表示论的其它概念.

进一步, 设 G 是有限群, $K = \mathbb{C}$ 是复数域. 根据第 3 章的结果, $\mathbb{C}$ 上每一个有特征标 χ_i 的不可约的 (或叫单的) G–模 (即 $\mathbb{C}[G]$–模) 同构于代数 $\mathbb{C}[G]$ 的某一个左理想 J_i (关于这一点见 §3 中的例 4). 若 $\dim_{\mathbb{C}}[G] = n_i$, 则 $\mathbb{C}[G]$ 含有 $\mathbb{C}[G]$–同构于 $J = J_{i,1}$ 的左理想的直和

$$A_i = J_{i,1} \oplus \cdots \oplus J_{i,n_i}.$$

在每一个左理想的同构类中取一个代表 J_i, 我们可以写出分解式

$$\mathbb{C}[G] = A_1 \oplus A_2 \oplus \cdots \oplus A_r, \tag{2}$$

它相应于群 G 的正则表示的分解式. 我们看到, 每一个分量 A_i 是唯一确定的.

现在若 J 是代数 $\mathbb{C}[G]$ 的极小左理想且 $t \in \mathbb{C}[G]$, 则 Jt 也是极小左理想 (可能是零理想). 于是由对应 $v \mapsto vt(v \in J)$ 确定的映射 $\varphi : J \to Jt$ 或是零映射或是 $\mathbb{C}[G]$–同构, 这是因为 $xv \in J$ (对任意 $x \in \mathbb{C}[G]$) 及 $\varphi(xv) = (xv)t = x(vt) = x\varphi(v)$. 由于这个原因, $J \subset A_i \Longrightarrow Jt \subset A_i, \forall t \in \mathbb{C}[G]$, 从而 A_i 是 $\mathbb{C}[G]$ 的双边理想. 分解式 (2) 是直和分解, 因此

$$i \neq j \Longrightarrow A_iA_j \subset A_i \cap A_j = 0.$$

我们打算根据第 3 章中所发展的特征标理论来获取关于分解 (2) 的更精确的信息. 首先来找出群代数 $\mathbb{C}[G]$ 的中心 $Z(\mathbb{C}[G])$. 根据定义

$$z \in Z(\mathbb{C}[G]) \Longleftrightarrow zg = gz \quad \forall g \in G.$$

若 $z = \sum\limits_{h \in G} \gamma_h h$, 则

$$\sum_{t \in G} \gamma_{g^{-1}t} t = g\left(\sum_h \gamma_h h\right) = \left(\sum_h \gamma_h h\right) g = \sum_{t \in G} \gamma_{tg^{-1}} t,$$

由此得到 $\gamma_{g^{-1}t} = \gamma_{tg^{-1}}, \forall t \in G$. 命 $t = gh$, 我们得到 $\gamma_h = \gamma_{ghg^{-1}}$. 这就是说

$$Z(\mathbb{C}[G]) = \langle K_1, K_2, \cdots, K_r \rangle_{\mathbb{C}},$$

其中

$$K_i = \sum_{g \in \mathcal{K}_i} g, \quad \mathcal{K}_i = g_i^G, \quad i = 1, 2, \cdots, r \tag{3}$$

($g_1, g_2, \cdots, g_r$ 是群 G 的共轭元类的代表). 易知 $K_1, \cdots, K_r$ 是线性无关元, 从而 $\dim_{\mathbb{C}} Z(\mathbb{C}[G]) = r$.

对于每一个元素 $a \in A_i$, 我们命它和按照规则 $L_a^{(i)}(v) = av, v \in J_i$ 作用在极小左理想 $J_i = J_{i,1}$ 上的线性变换 $L_a^{(i)}$ 相对应. 因为显然有

$$L_{\lambda a}^{(i)} = \lambda L_a^{(i)}, \quad L_{a+b}^{(i)} = L_a^{(i)} + L_b^{(i)}, \quad L_{ab}^{(i)} = L_a^{(i)} L_b^{(i)},$$

所以 $\varphi : a \mapsto L_a^{(i)}$ 是代数 A_i 到自同态代数 $\mathrm{End}_{\mathbb{C}} J_i \cong M_{n_i}(\mathbb{C})$ 的同态. 假定 $0 \neq a \in \mathrm{Ker}\,\varphi$, 即 $aJ_i = 0$. 所有左理想 $J_{i,j}$ 都是 $\mathbb{C}[G]$–同构的, 且若 $\varphi_j : J_i \to J_{i,j}$ 是同构, 则

$$aJ_{i,j} = a\varphi_j(J_i) = a\varphi_j(eJ_i) = \varphi_j(aeJ_i) = \varphi_j(0) = 0.$$

这就是说, $aA_i = aJ_{i,1} + \cdots + aJ_{i,n_i} = 0$, 而在这种情形, 也有 $a\mathbb{C}[G] = 0$, 这是因为对所有 $j \neq i$, 有 $a \in A_i \Longrightarrow aA_j = 0$. 然而 $ae = a \neq 0$. 所得到的矛盾表明 $\mathrm{Ker}\,\varphi = 0$. 于是 φ 是单同态, 而因为 $\dim A_i = n_i^2 = \dim M_{n_i}(\mathbb{C})$, 所以 $A_i \overset{\varphi}{\cong} M_{n_i}(\mathbb{C})$. 考虑到命题 2, 我们得到下面关于群代数 $\mathbb{C}[G]$ 的结构的定理.

定理 4 有限群 G 在复数域 $\mathbb{C}$ 上的群代数 $\mathbb{C}[G]$ 分解成与全阵代数同构的单的双边理想的直和 (2):

$$\mathbb{C}[G] \cong M_{n_1}(\mathbb{C}) \oplus M_{n_2}(\mathbb{C}) \oplus \cdots \oplus M_{n_r}(\mathbb{C}).$$

特别地, n 阶交换群在 $\mathbb{C}$ 上的群代数和域 $\mathbb{C}$ 的 n 个拷贝的直和同构.

推论 (伯恩赛德 (Burnside) 定理) 设 Φ 是有限群 G 在 $\mathbb{C}$ 上的 n 次不可约矩阵表示. 则在矩阵 Φ_g 当中有 n^2 个线性无关的, 即 $\langle \Phi_g | g \in G\rangle_{\mathbb{C}} = M_n(\mathbb{C})$. □

中心 $Z(\mathbb{C}[G])$, 作为 $\mathbb{C}[G]$ 的交换子代数, 其结构完全由关系式

$$K_i K_j = \sum_{s=1}^{r} n_{ij}^s K_s \tag{4}$$

中的整数 n_{ij}^k 确定. 这些数叫做**结构常数**. 由于有了 K_i 的表达式 (3), 易知 n_{ij}^s 是使 $gh = g_s \in \mathcal{K}_s$ 的偶 (g, h) $(g \in \mathcal{K}_i, h \in \mathcal{K}_j)$ 的个数. 在 $Z(\mathbb{C}[G])$ 中取另一基

$$I_i = \frac{n_i}{|G|} \sum_{s=1}^{r} \overline{\chi_i(g_s)} K_s = \frac{n_i}{|G|} \sum_{g \in G} \overline{\chi_i(g)} g, \quad 1 \leqslant i \leqslant r. \tag{5}$$

和第 3 章 §5 中一样, 这里 $\chi_1, \cdots, \chi_r$ 是不可约表示的特征标, $n_1, \cdots, n_r$ 是它们的次数. 按公式

$$K_s = |\mathcal{K}_s| \sum_{i=1}^{r} \frac{\chi_i(g_s)}{n_i} I_i$$

可以完成相反的转变. 为了证实这一点, 需要利用第 3 章 §5 中的关系式 (4), 它指出

$$\sum_{i=1}^{r} I_i = \frac{1}{|G|} \sum_{g \in G} g \sum_i n_i \overline{\chi_i(g)} = \frac{1}{|G|} \sum_{g \in G} g \sum_i \chi_i(e) \overline{\chi_i(g)} = \frac{1}{|G|} e |C_G(e)| = e.$$

进一步, 利用第 3 章 §4 习题 1 中的广义正交关系, 我们得到

$$\begin{aligned} I_i I_j &= \frac{n_i n_j}{|G|^2} \sum_{g,t \in G} \overline{\chi_i(g)}\, \overline{\chi_j(t)}\, gt = \frac{n_i n_j}{|G|} \sum_{h \in G} \left\{ \frac{1}{|G|} \sum_{g \in G} \overline{\chi_i(g)} \chi_j(hg) \right\} h^{-1} \\ &= \frac{n_i n_j}{|G|} \frac{\delta_{ij}}{n_i} \sum_{h \in G} \chi_j(h) h^{-1} = \delta_{ij} I_j. \end{aligned}$$

因此, 根据公式 (5) 算出的中心元 I_i 满足关系式

$$\begin{aligned} &e = I_1 + I_2 + \cdots + I_r \\ &I_i^2 = I_i, \quad I_i I_j = 0, \quad i \neq j. \end{aligned} \tag{6}$$

并且由于这个原因, 这些 I_i 叫做群代数 $\mathbb{C}[G]$ 的**中心正交幂等元**. 关系式 $e = I_1 + \cdots + I_r$ 是这个组的完备性条件. 命 $B_i = I_i\mathbb{C}[G]$, 我们立即发现, B_i 是 $\mathbb{C}[G]$ 的双边理想, 有单位元 I_i, 并且有直和分解

$$\mathbb{C}[G] = B_1 \oplus B_2 \oplus \cdots \oplus B_r. \tag{7}$$

由 (5) 直接推出

$$\chi_j(I_i) = n_i \frac{1}{|G|} \sum_g \overline{\chi_i(g)}\chi_j(g) = n_i\delta_{ij}.$$

因此, B_i 包含对应于特征标 χ_i 的极小左理想 $J \subset A_i$. 因为 A_i 和 B_i 都是双边理想, 所以 $A_i \subset B_i$. 将分解式 (2) 和 (7) 比较一下, 我们得到 $A_i = B_i$. 这样就证明了定理 3 的改进了的变体.

定理 5 *可根据公式 (5) 算出的元素 $I_i, 1 \leqslant i \leqslant r$ 形成有限群 G 的群代数 $\mathbb{C}[G]$ 的中心正交幂等元完备组. 直和分解*

$$\mathbb{C}[G] = I_1\mathbb{C}[G] \oplus I_2\mathbb{C}[G] \oplus \cdots \oplus I_r\mathbb{C}[G]$$

中同构于全阵代数 $M_{n_i}(\mathbb{C})$ 的单分量 $I_i\mathbb{C}[G]$ 含有所有对应于特征标 χ_i 的极小左理想.

从韦德伯恩–阿廷定理 (见第 1 段) 及群代数的一般结构理论 (在定理 3 中表述出的对于有限群的终结性结论) 出发, 可以发展出整个群表示理论. 我们曾经朝着相反的方向走过, 本质上只根据了舒尔引理.

最后, 我们来证明关于不可约表示的次数及特征标的值的两个有益的断言.

定理 6 *有限群 G 在 $\mathbb{C}$ 上的不可约表示 (Φ, V) 的次数 n 整除阶 $|G|$.*

证明 设 $\widetilde{\Phi}$ 是群代数 $\mathbb{C}[G]$ 的相应表示. 根据舒尔引理 (§3 中的命题 2), 和所有 $\Phi(g)(g \in G)$ 可交换从而属于 $\mathrm{End}_{\mathbb{C}[G]}(V)$ 的线性变换 $\widetilde{\Phi}(K_i)$ 应该是恒等变换的倍数: $\widetilde{\Phi}(K_i) = \omega_i\mathcal{E}$. 我们有

$$n\omega_i = \mathrm{tr}\,\omega_i\mathcal{E} = \mathrm{tr}\widetilde{\Phi}(K_i) = \sum_h \mathrm{tr}\Phi(hg_ih^{-1}) = |\mathcal{K}_i|\chi_\Phi(g_i),$$

由此得到

$$\omega_i = \frac{|\mathcal{K}_i|\chi_\Phi(g_i)}{n}.$$

将 $\widetilde{\Phi}$ 应用于关系式 (4), 我们得到

$$\omega_i\omega_j = \sum_{k=1}^r n_{ij}^k \omega_k.$$

于是 $\mathbb{Z}[\omega_i]$ 是有限型 $\mathbb{Z}$–模 $\mathbb{Z}[\omega_1,\cdots,\omega_r]$ 的子模, 并且根据 §3 第 3 目中的结果, ω_i 是代数整数. 根据这个理由,

$$\frac{|G|}{n}=\frac{|G|}{n}(\chi_\Phi|\chi_\Phi)G=\frac{1}{n}\sum_g\chi_\Phi(g)\overline{\chi_\Phi(g)}$$
$$=\frac{1}{n}\sum_{i=1}^r|\mathcal{K}_i|\cdot\chi_\Phi(g_i)\overline{\chi_\Phi(g_i)}=\sum\omega_i\overline{\chi_\Phi(g_i)}$$

是代数整数. 这就是说, $|G|/n\in\mathbb{Z}$. □

引理 2 设 A 是循环群且 χ 是它的特征标, 可能是可约的. 命 $S=\{a\in A|A=\langle a\rangle\}$. 假定 $\chi(s)\neq 0,\forall s\in S$. 则

$$\sum_{s\in S}|\chi(s)|^2\geqslant|S|.$$

证明 设 $n=|A|$ 且 F 是多项式 X^n-1 在 $\mathbb{Q}$ 上的分裂域. 下一章中将研究伽罗瓦群 $G=\mathrm{Gal}F/\mathbb{Q}$ 及 G 在特征标上的作用. 为了明显起见, 我们用指数形式来表达这个作用. 若 $\sigma\in G$ 且 ζ 是 1 的一个 n 次根, 则 $\zeta^\sigma=\zeta^m$, 其中 g. c. d $(m,n)=1$. 进一步, $\chi(s)=\zeta_1+\cdots+\zeta_k,\zeta_i^n=1$, 并且根据定义,

$$\chi^\sigma(s)=\zeta_1^m+\cdots+\zeta_k^m=\chi(s^m).$$

群 G 是交换群且 $\alpha\mapsto\overline{\alpha}\,(\alpha\in F)$ 也是 G 中元素, 于是 $\overline{\alpha^\sigma}=(\overline{\alpha})^\sigma,\alpha\in F,\sigma\in G$. 因此,

$$|\alpha^\sigma|^2=\alpha^\sigma\overline{\alpha^\sigma}=\alpha^\sigma(\overline{\alpha})^\sigma=(\alpha\overline{\alpha})^\sigma=(|\alpha|^2)^\sigma,$$
$$(|\chi(s)|^2)^\sigma=|\chi(s^m)|^2,\quad \mathrm{g.c.d}(m,n)=1$$

(m 只依赖于 σ).

我们看到, 若 $\mathrm{g.c.d}(m,n)=1$, 则 $s\in S\Longrightarrow s^m\in S$. 此外, $x\mapsto x^m$ 是 A 上的双射, 它是置换. 这就是说, $\prod_{s\in S}|\chi(s)|^2$ 对 G 不变, 因此它是有理数. 同时它是代数整数, 因此, 这个数应该在 $\mathbb{Z}$ 中. 根据条件 $\chi(s)\neq 0$, 所以 $\prod_{s\in S}|\chi(s)|^2\geqslant 1$. 但是, 对任意正实数 $r_1,\cdots,r_k$ 有

$$\frac{1}{k}\sum_{i=1}^k r_i\geqslant\left(\prod_i r_i\right)^{1/k}.$$

在我们的情形,

$$\frac{1}{|S|}\sum_{s\in S}|\chi(s)|^2\geqslant 1.$$ □

定理 7 (W. 伯恩赛德) 设 G 是有限群, $\chi\in\mathrm{Irr}(G)$. 若 $\chi(e)>1$, 则至少有一个 $g\in G$ 使 $\chi(g)=0$.

证明 G 中两个元素叫做等价的, 若它们生成 G 的同一个循环子群. 这样我们就把 G 分成了类. 假定对任何 $g \in G$, 都有 $\chi(g) \neq 0$. 则根据引理 2, 对每一个等价类 S 都有

$$\sum_{s\in S} |\chi(s)|^2 \geqslant |S|.$$

按所有类中的非单位元的元素相加, 我们得到不等式

$$\sum_{g\neq e} |\chi(g)|^2 \geqslant |G| - 1.$$

因此,

$$|G| = \sum_{g\in G} |\chi(g)|^2 \geqslant |G| - 1 + \chi(e)^2,$$

由此得到 $\chi(e) \leqslant 1$, 矛盾. □

推论 若群 G 和它自己的换位子群 G 相等, 则

$$|G| \cdot \prod_{i=1}^{r} K_i = \left(\prod_{i=1}^{r} |\mathcal{K}_i|\right) \sum_{l=1}^{r} K_l \tag{8}$$

(即 $\mathbb{Q}[G]$ 中的中心元 $\prod\limits_i K_i$ 和 $\sum\limits_i K_i$ 成比例).

证明 设 $g_1, \cdots, g_r$ 是共轭类 $\mathcal{K}_1, \cdots, \mathcal{K}_r$ 的代表, $K_1, \cdots, K_r$ 是 $\mathcal{K}_1, \cdots, \mathcal{K}_r$ 中的元素之和. 我们知道 (见 (4))

$$K_i K_j = \sum_{l=1}^{r} n_{ij}^{l} K_l,$$

$$\omega(K_i)\omega(K_j) = \sum_{l} n_{ij}^{l} \omega(K_l),$$

其中 $\omega(K_i) = \chi(g_i)|\mathcal{K}_i|/\chi(e)$ 是代数整数. 用 $\overline{\chi(g_s)}$ 乘关系式

$$\frac{\chi(g_i)\chi(g_j)}{\chi(e)} |\mathcal{K}_i||\mathcal{K}_j| = \sum_{l} n_{ij}^{l} \chi(g_l)|\mathcal{K}_l|$$

的两边, 并按 χ 相加, 我们得到结构常数的公式

$$n_{ij}^{s} = \frac{|\mathcal{K}_i||\mathcal{K}_j|}{|G|} \sum_{\chi} \frac{\chi(g_i)\chi(g_j)\overline{\chi(g_s)}}{\chi(e)}. \tag{9}$$

和 (9) 相类似, 命

$$\prod_{i=1}^{r} K_i = \sum_{l=1}^{r} N_l K_l,$$

我们将有

$$\frac{\chi(g_1)\cdots\chi(g_r)\prod_{i=1}^{r}|\mathcal{K}_i|}{\chi(e)^{r-1}}=\sum_{l=1}^{r}N_l\chi(g_l)|\mathcal{K}_l|,$$

于是

$$N_s=\frac{\prod_i|\mathcal{K}_i|}{|G|}\sum_{\chi}\frac{\chi(g_1)\cdots\chi(g_r)\overline{\chi(g_s)}}{\chi(e)^{r-1}}. \tag{$*$}$$

现在若 $G=G'$, 则除了 1_G 以外, 所有特征标的次数都大于 1 (第 3 章 §5 中的定理 5) 并且根据定理 6, 当 $\chi\neq 1_G$ 时, $\chi(g_1)\chi(g_2)\cdots\chi(g_r)=0$. 由公式 $(*)$ 直接得到 $N_s=\dfrac{\prod_i|\mathcal{K}_i|}{|G|}\cdot 1, \forall s$, 这就是我们所要的. □

注 设 A 是域 P 上任意维数的任意一个 (即未必是结合的) 代数. 对于每三个元素 $x,y,z\in A$, 我们命它对应一个叫做它们的**结合子**的表达式 $(x,y,z)=(xy)z-x(yz)$. 根据与结合子或其它表达式相联系的恒等关系式, 可以得到不同类型 (还有别的叫法, **本原类, 流形**) 的代数. 例子有:

1) **结合代数** $(x,y,z)=0$;

2) **交错代数** $(x,x,y)=0=(y,x,x)$;

3) 若尔当 (Jordan) **代数** $(x,y,x^2)=0$, $xy-yx=0$.

显然, 沿着这种公理化的道路可以无限制地走下去. 然而奇妙的是, 许多非结合代数类自然地出现在远离代数学的科学领域. 作为最鲜明的例子的应该提到若尔当代数, 正像 [BA II] 中所提到的, 它从量子力学来到数学 (来自物理学家 Jordan); 以及李 (Lie) 代数, 它原先只是为了描述 (在确定的条件下) 拓扑群的局部结构的 (索福斯 · 李 (Sophus Lie)——19 世纪最伟大的数学家之一). 本书已经谈到了李代数, 在下一节中将再一次提到它们.

习 题

1. 广义四元数代数. 证明: 用乘法表

$\cdot$	1	e_1	e_2	e_3
1	1	e_1	e_2	e_3
e_1	e_1	n	e_3	ne_2
e_2	e_2	$-e_3$	m	$-me_1$
e_3	e_3	$-ne_2$	me_1	$-nm$

(其中 $n,m\in\mathbb{Z}, nm\neq 0$) 可以在 $\mathbb{Q}$ 上四维向量空间 $\mathbb{H}(n,m)=\langle 1,e_1,e_2,e_3\rangle_{\mathbb{Q}}$ 中引入含单

位元的结合代数的结构. 为了这个目的, 利用表示

$$x = x_0 + x_1e_1 + x_2e_2 + x_3e_3 \mapsto A_x = \begin{pmatrix} x_0 + x_1\sqrt{n} & x_2\sqrt{m} + x_3\sqrt{nm} \\ x_2\sqrt{m} - x_3\sqrt{nm} & x_0 - x_1\sqrt{n} \end{pmatrix}.$$

行列式 $\det A_x = x_0^2 - x_1^2n - x_2^2m + x_3^2nm$ 叫做**元素 x 的范数**. 验证, 当满足 " $x \in \mathbb{H}(n,m), x \neq 0 \Longrightarrow N(x) \neq 0$ " 这一条件时, 空间 $\mathbb{H}(n,m)$ 是可除代数 (**广义四元数代数**). 利用 §2 习题 7 中的概念及结果, 证明: 对于素数 $p \equiv \pm 3 (\bmod 8)$, 代数 $\mathbb{H}(2,p)$ 将是可除代数.

2. 设 A 是 $\mathbb{R}$ 上含单位元 1 的代数. 设在 A 中给定了共轭运算 $x \mapsto \overline{x}$, 它具有性质 $\overline{\overline{x}} = x, \overline{xy} = \overline{y}\overline{x}$. 我们给予空间 $A \oplus A = \{(x,y)|x,y \in A\}$ 一个双线性的乘法运算

$$(x,y)(u,v) = (xu - \overline{v}y, y\overline{u} + vx).$$

得到一个代数, 它叫做**代数 A 的加倍**.

验证: $\mathbb{C}$ 是代数 $\mathbb{R}$ 的加倍, 而 $\mathbb{H}$ 是代数 $\mathbb{C}$ 的加倍. 代数 $\mathbb{H}$ 的加倍叫做**凯莱代数** $\mathbb{C}a$.

验证: $\mathbb{C}a$ 是非交换的和非结合的代数. 以明显的形式表达出 $\mathbb{C}a$ 中的共轭运算.

3. 将 $\mathbb{F}_{2^n}$ 看作 $\mathbb{F}_2$ 上 n 维向量空间 V. 和从 $\mathbb{F}_{2^n}$ 继承来的加法运算同时, 在 V 中引入乘法运算 $(x,y) \mapsto x \circ y = \sqrt{xy}$, 其中 $x \mapsto \sqrt{x}$ 是 $\mathbb{F}_{2^n}$ 的自同构, 它和 $x \mapsto x^2$ 相逆, 因此 $\sqrt{x+y} = \sqrt{x} + \sqrt{y}$. 证明: $(V, +, \circ)$ 是 $\mathbb{F}_2$ 上交换 (非结合) 代数, 它具有性质: a) V 中没有零因子, 也没有单位元; b) 方程 $a \cdot x = b$ (其中 $a \neq 0$) 唯一地可解; c) 自同构群 $\mathrm{Aut}(V)$ 传递地作用在 $V \backslash \{0\}$ 上.

4. 在任意代数中, 结合子总满足

$$t(x,y,z) + (t,x,y)z = (tx,y,z) - (t,xy,z) + (t,x,yz).$$

用直接检验来证实它, 并证明: 若域 P 上有单位元 1 的代数 A 中, 对所有结合子都有 $(x,y,z) \in P \cdot 1$, 则 A 是结合代数.

5. 设 G 及 H 是有限群且 $\mathbb{C}[G] \cong \mathbb{C}[H]$ 是 $\mathbb{C}$–代数同构, 能否断言 $G \cong H$?

6. 设 Φ 是有限群 G 的 n 次不可约复矩阵表示. 证明: 若常数 $(n \times n)$–矩阵 C 满足

$$\mathrm{tr}\{C\Phi_x\} = 0 \quad \forall x \in G,$$

则 $C = 0$.

§5 李代数 $\mathfrak{sl}(2)$ 上的不可约模

1. 起初的材料　我们回忆起, 域 P 上李代数 L 中元素 $x, y \in L$ 的积习惯上记作 $[x,y]$ 或更简单地记作 $[xy]$. 根据李代数的定义, 双线性运算 $(x,y) \mapsto [xy]$ 满足两个要求:

i) $[xx] = 0$　($[xy] = -[yx]$——**反交换性**);

ii) $[[xy]z]+[[yz]x]+[[zx]y]=0$ (**雅可比恒等式**).

我们也从 [BA II] 知道, 若 A 是域 P 上结合代数, 则命 $[xy]=xy-yx$ (两个元素的换位子) 时可以对向量空间 A 给出李代数 $L(A)$ 的结构.

特别地, 设 $A=\mathrm{End}_P(V)=\mathfrak{L}(V)$ 是 P 上有限维向量空间 V 的所有线性变换组成的代数. 任意同态

$$\varphi: L\to L(\mathfrak{L}(V))$$

叫做李代数 L 的表示. 相应于前一节中的术语, 表示空间 V 也叫做 L-模 (或李代数 L 上模). L-模由三个公理形式地给出:

L1) $x(\alpha u+\beta v)=\alpha xu+\beta xv$;

L2) $(\alpha x+\beta y)v=\alpha xv+\beta yv$;

L3) $[xy]v=x(yv)-y(xv)$.

实际上每一个 L-模是泛包络代数 $U(L)$ (即由 L 生成的结合代数) 上的模 (关于这一点, 我们不表述伯克霍夫–维特 (Birkhoff-Witt) 定理了).

例 1 域 P 上任意代数 A (未必是结合的) 的微分是指环 $(A,\cdot)$ 的微分 $\mathcal{D}$:

$$\mathcal{D}(u+v)=\mathcal{D}(u)+\mathcal{D}(v),\quad \mathcal{D}(u\cdot v)=\mathcal{D}(u)\cdot v+u\mathcal{D}(v), u,v\in A,$$

它和 P 中常数进行运算时可交换: $\mathcal{D}(\lambda u)=\lambda\mathcal{D}(u),\lambda\in P, a\in A$. 乘法

$$[\mathcal{D}_1\mathcal{D}_2]=\mathcal{D}_1\mathcal{D}_2-\mathcal{D}_2\mathcal{D}_1$$

赋予所有微分组成的集合 $\mathrm{Der}(A)$ (它是 P 上向量空间) 以李代数的结构.

特别地, 若 $A=P[X]$ 是多项式代数, 则 $\mathrm{Der}(A)$ 由按规则

$$\mathcal{D}_u(f)=u\frac{df}{dX}=uf'$$

作用的微分 $\mathcal{D}_u(u\in A)$ 组成. 根据定义

$$\begin{aligned}[\mathcal{D}_u,\mathcal{D}_v](f)&=\mathcal{D}_u(\mathcal{D}_vf)-\mathcal{D}_v(\mathcal{D}_uf)=\mathcal{D}_u(vf')-\mathcal{D}_v(uf')\\&=u(vf')'-v(uf')'=u(v'f'+vf'')-v(u'f'+uf'')=(uv'-u'v)f'.\end{aligned}$$

因此,

$$[\mathcal{D}_u\mathcal{D}_v]=\mathcal{D}_{uv'-u'v}.$$

于是我们看到, 代数 $\mathrm{Der}(A)$ 同构于有基础空间 A 及乘法 $[uv]=uv'-u'v$ 的无限维李代数 $(A,[**])$. 命 $A_{(i)}=\langle X^{i+1}\rangle_P$, 我们得到 A 的直和分解

$$A=A_{(-1)}\oplus A_{(0)}\oplus A_{(1)}\oplus A_{(2)}\oplus\cdots,$$

它具有**分次李代数**的性质

$$[A_{(i)},A_{(j)}]\subset A_{(i+j)}$$

(和 §4 第 1 目中的例 2 作比较). 李代数 $(K, [*, *])$ 用两种方法作用在向量空间 K 上: 1) $(a, f) \mapsto af'$ (自然的作用); 2) $(a, f) \mapsto af' - a'f$ (添加自同态的作用). 结果得到两个不同构的 $(A, [* \, *])$–模.

例 2　迹为零的斜埃尔米特矩阵组成的三维实空间

$$\mathfrak{su}(2) = \langle \mathbf{k}_1, \mathbf{k}_2, \mathbf{k}_3 \rangle_{\mathbb{R}}$$

被赋予李代数的结构. 关系式

$$[\mathbf{k}_1 \mathbf{k}_2] = \mathbf{k}_3, \quad [\mathbf{k}_2 \mathbf{k}_3] = \mathbf{k}_1, \quad [\mathbf{k}_3 \mathbf{k}_1] = \mathbf{k}_2$$

丝毫不差地重复了 $\mathbb{R}^3$ 中向量的向量积规则.

从紧群表示的一般理论推出, 在群 SU(2) 的不可约表示和它的李代数 $\mathfrak{su}(2)$ 的不可约表示之间有互相单值的对应. 在直觉上, 这一点是可以理解的, 只要注意到群表示的连续性并看到在算子 $\Phi(g_t)$ (其中 g_t 是群 SU(2) 中按微分方式依赖于 $t \in \mathbb{R}$ 的元素; $g_0 = e$) 的线性包络中, 线性算子 $d\Phi(g_t)/dt|_{t=0}$ 已经被包含在代数 $\mathfrak{su}(2)$ 中. 为了证实已在第 3 章 §6 中得到的群 SU(2) 的不可约表示的完全描写, 我们需要证实, 对于任意自然数 $n, \mathbb{C}$ 上 n 维不可约 $\mathfrak{su}(2)$–模精确到同构只有一个. 为了达到这个目的, 从开始时的实李代数 $\mathfrak{su}(2)$ 转向它的和所有迹为零的复 $2 \otimes 2$–矩阵组成的李代数 $L = \mathfrak{sl}(2) = \mathfrak{su}(2) \otimes_{\mathbb{R}} \mathbb{C}$ 一致的 "复化" 是合适的. 代数 L 的基元素

$$e_{-1} = \mathbf{k}_1 - i\mathbf{k}_2, \quad e_0 = 2i\mathbf{k}_3, \quad e_1 = \mathbf{k}_1 + i\mathbf{k}_2$$

按规则

$$[e_{-1} e_1] = e_0, \quad [e_0 e_{-1}] = -2e_{-1}, \quad [e_0 e_1] = 2e_1 \tag{1}$$

相乘. 暂时忘掉 L 的来历, 可以认为 $L = \langle e_{-1}, e_0, e_1 \rangle$ 是有乘法表 (1) 的 $\mathbb{C}$ 上抽象三维李代数. 容易验证, L 是单李代数. 于是它的任意一个维数 > 1 的不可约模都是忠实的.

2. 权及重数　首先设 $V \neq 0$ 是 $\mathbb{C}$ 上任意有限维 L–模, 并设 E_{-1}, E_0, E_1 是分别对应于元素 e_{-1}, e_0, e_1 的 V 的线性变换 (或在固定基下的矩阵). 在李代数的表示论中已经建立了自己的术语, 我们将照样使用.

定义　V 的有特征值 $\lambda \in \mathbb{C}$ 的线性变换 E_0 的特征子空间

$$V^\lambda = \{v \in V | E_0 v = \lambda v\}$$

习惯上叫做有**权** λ 的向量组成. 维数 $\dim V^\lambda$ 叫做**权 λ 的重数**.

引理 1 若 $v \in V^\lambda$, 则

$$E_1 v \in V^{\lambda+2}, \quad E_{-1} v \in V^{\lambda-2}$$

(E_1 是 **"提高" 算子**, 而 E_{-1} 是 **"降低" 算子**).

证明 根据公理 L3), 我们有

$$E_0(E_1 v) = [E_0 E_1]v + E_1(E_0 v) = 2E_1 v + E_1(\lambda v) = (\lambda+2)E_1 v,$$

因此根据定义, $E_1 v \in V^{\lambda+2}$. 类似地,

$$E_0(E_{-1}v) = (\lambda-2)E_{-1}v. \qquad \square$$

3. 最高权向量 由 [BA II] 知道, 对应于不同特征值的向量是线性无关的. 因此和

$$W = \sum_\lambda V^\lambda \subset V$$

是直和. 由引理 1 还推出 W 是 V 的 L–子模. 因为 $W \neq 0$, 所以在 L–模 V 不可约的情形应该有等式 $W = V$.

定义 向量 $v_0 \in V$ 叫做**权为 λ 的最高向量**, 若 $v_0 \neq 0$, 且

$$E_1 v_0 = 0, \quad E_0 v_0 = \lambda v_0.$$

引理 2 任意有限维 L–模 V 有最高权向量.

证明 取任意一个权为 μ 的向量 $v(\neq 0)$ 并建立权为 $\mu, \mu+2, \mu+4, \cdots$ 的向量序列 $v, E_1 v, E_1^2 v, \cdots$ (见引理 1). 因为 $\dim V < \infty$, 所以对某个 m, 有 $E_1^{m+1} v = 0$. 取 m 为极小的, 我们可以命 $v_0 = E_1^m v, \lambda = \mu + 2^m$. $\square$

引理 3 设 V_n 是 $\mathbb{C}$ 上 $n+1$ 维向量空间, 它有选定的基 $(v_0, v_1, \cdots, v_n)$, E_{-1}, E_0, E_1 是由公式

$$\begin{aligned} E_{-1} v_m &= (m+1) v_{m+1}, \\ E_0 v_m &= (n-2m) v_m, \\ E_1 v_m &= (n-m+1) v_{m-1} \end{aligned} \tag{2}$$

确定的线性变换, 其中 $v_{-1} = 0 = v_{n+1}$. 则 V_n 是不可约 L–模.

证明 直接验证得出, 和乘法表 (1) 及 L–模公理一致的关系式

$$\begin{aligned} E_1(E_{-1}v_m) - E_{-1}(E_1 v_m) &= E_0 v_m, \\ E_0(E_{-1}v_m) - E_{-1}(E_0 v_m) &= -2E_{-1} v_m, \\ E_0(E_1 v_m) - E_1(E_0 v_m) &= 2E_1 v_m \end{aligned}$$

成立. 因为 $E_1v_0 = (n+1)v_{-1} = 0, E_0v_0 = nv_0$, 所以 v_0 是权为 n 的最高权向量, 而整个空间 V_n 可以写成一维权子空间 $V^{n-2m} = \langle v_m \rangle$ (每一个权有重数 1) 的直和的形状:

$$V_n = V^n \oplus V^{n-2} \oplus \cdots \oplus V^{-n}.$$

假定 V_n 中存在子模 $U \neq 0$, 我们取线性变换 E_0 的任意一个特征向量 $u \in U$. 根据分解式 (3), 对某个 m, 有 $u = \lambda v_m$. 连续不断地应用提高算子 E_1 (见公式 (2)), 我们得到 $v_{m-1} \in U, \cdots, , v_0 \in U$, 而利用降低算子 E_{-1}, 我们从最高权向量 v_0 得到所有其余的向量. 这就是说, $U = V_n$, 从而 V_n 是不可约 L-模. □

我们看到, V_0 是平凡 (一维的) 模, 而 V_1 是对应于代数 L 的自然定义的模: 在基 (v_0, v_1) 下, 线性变换 E_{-1}, E_0, E_1 有它们自己的矩阵

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

4. 分类的结果 下面的定理解决了摆在我们面前的问题.

定理 1 每一个 $\mathbb{C}$ 上 $n+1$ 维不可约 L-模 V 同构于 V_n.

证明 根据引理 2, 我们的模 V 有某一个权为 λ 的最高权向量 v_0. 命

$$v_{-1} = 0, \quad v_m = \frac{1}{m!}E_1^m v_0 = \frac{1}{m!}E_{-1}(\cdots(E_{-1}v_0)\cdots), \text{ 当 } m \geqslant 0.$$

我们断言, 对任意 $m \geqslant 0$, 公式

$$\begin{aligned} E_{-1}v_m &= (m+1)v_{m+1}, \\ E_0v_m &= (\lambda - 2m)v_m, \\ E_1v_m &= (\lambda - m + 1)v_{m-1} \end{aligned} \tag{2'}$$

成立.

事实上, 当 $m = 0$ 时, 公式 (2′) 归结为最高权向量 v_0 及向量 v_1 的定义, 接下去我们对 m 用归纳法.

a) 用公式 $E_{-1}v_m = (m+1)v_{m+1}$ 确定向量 v_{m+1}.

b) 公式 $E_0v_m = (\lambda - 2m)v_m$ 由引理 1 推出.

c) 若已经知道 $E_1v_{m+1} = (\lambda - m + 2)v_{m-2}$, 则在等式

$$\begin{aligned} mE_1v_m &= E_1(E_{-1}v_{m-1}) = [E_1E_{-1}]v_{m-1} + E_{-1}(E_1v_{m-1}) \\ &= E_0V_{m-1} + (\lambda - m + 2)E_{-1}v_{m-2} \\ &= \{(\lambda - 2m + 2) + (\lambda - m + 2)(m - 1)\}v_{m-1} = m(\lambda - m + 1)v_{m-1}. \end{aligned}$$

的两边约掉 m 以后就得到公式 (2′) 中的最后一个.

若对某个 r, 向量 $v_0, v_1, \cdots, v_r$ 都不为零, 则因为有不同的权, 它们应该是线性无关的. 另一方面, 由于 V 的不可约性, 由 v_0 生成的子模和 V 相等, 而因为 $\dim V = n+1$, 所以 $V = \langle v_0, v_1, \cdots, v_n\rangle$ 而 $v_{n+1} = v_{n+2} = \cdots = 0$. 特别地,

$$0 = E_1 v_{n+1} = (\lambda - n)v_n = 0 \Longrightarrow \lambda = n.$$

(我们注意到很有意思的蕴涵 $\dim V < \infty \Longrightarrow \lambda \in \mathbb{Z}, \lambda \geqslant 0$).

将值 $\lambda = n$ 代入公式 (2′), 并考虑到所选记号, 实际上我们得到了确定 (根据引理 3) 不可约 L-模 V_n 的公式 (2). 这就是说 $V \cong V_n$. □

习 题

1. 回到基元素

$$\mathbf{k}_1 = \frac{1}{2}(e_{-1} + e_2), \quad \mathbf{k}_2 = \frac{i}{2}(e_{-1} - e_1), \quad \mathbf{k}_3 = -\frac{i}{2}e_0,$$

并利用公式 (2), 再将它们和线性变换 K_1, K_2, K_3 相对应, 用此给予 V_n 以 $\mathfrak{su}(2)$-模结构.

2. 设 $L = \langle e_{-1}, e_0, e_1\rangle$ 是特征 $p > 2$ 的代数闭域 F 上有乘法表 (1) 的单李代数. 考虑 p 阶方阵

$$E_{-1} = \begin{pmatrix} 0 & \gamma_1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \gamma_2 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & \gamma_{p-2} & 0 \\ 0 & 0 & 0 & \cdots & 0 & \gamma_{p-1} \\ \gamma_0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}, \quad E_1 = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & \beta \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

$$E_0 = [E_{-1}E_1] = \mathrm{diag}(\lambda, \lambda+2, \cdots, \lambda+2(p-2), \lambda+2(p-1)).$$

验证, 对应 $e_i \mapsto E_i (i = -1, 0, 1)$ 确立了李代数 L 的依赖于三个参数 $(\lambda, \beta, \gamma_0)$ 的不可约矩阵表示. 并且

$$\gamma_k = \beta\gamma_0 + k\lambda + k(k-1), \quad k = 1, 2, \cdots, p-1.$$

(这一完全新的情况对于有限特征域上的表示是典型的).

第 5 章 伽罗瓦理论初步

本章除介绍了关于域的有限扩张, 特别是关于有限域和代数数域的初步知识以外, 还介绍了伽罗瓦理论的片断, 它对于证明次数大于 4 的代数方程不能用根式解的经典定理已足够用. 也证明了更有意思的数论事实. 还阐述了伽罗瓦理论的现代方向的初步, 它吸引我们之处是可以在第 3 章的初等水平上充分地利用特征标理论.

§1 域的有限扩张

1. 本原元素和扩张的次数 若 F 是包含子域 P 的域, 则 F 也叫做**域 P 的扩张** ([BA I], 第 4 章, § 3). 首先我们限于当扩张 $F = P(\theta)$ 是在域 P 上添加 (在给定域 F 里边) 一个元素 $\theta \in F$ 而得到的最简单的情形. 称 $P(\theta)$ 是域 P 的**单扩张**, 而 θ 是这个扩张的**本原元素**. 按照自身的意义, $P(\theta)$ 是整环 $P[\theta]$ 的分式域. 元素 θ 在 P 上是**超越的**当且仅当扩张 $P(\theta)$ 和 $P[X]$ 的有理分式域同构. 然而, 如果 θ 是代数元, 则 $P(\theta) \cong P[X]/(f(X))$ (第 4 章, § 1, 定理 2), 这里 $f(X)$ 是次数 $n > 0$ 的不可约多项式, θ 是它的根. 反之, 若 $f(X)$ 是不可约多项式, 则正如我们从第 4 章知道的, 可以以经典的方式构造一个域 F 使得 f 在其中至少有一个根 (我们将它叫做 θ). 根据构造, 明显知道 F 和形如

$$a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}, \quad a_i \in P, \quad n = \deg f$$

的元素所作成的集合相同.

对于环 $P[\theta]$ 的元素来说, 这是明显的 (作带余除法以 $f(X)$ 除 $g(X)$, 并作代入 $X = \theta$); $P[\theta]$ 中的除法是这样来实现的: 若 $g(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$, 则 f 的不可约性导致 $\mathrm{g.c.d}(f, g) = 1$, 并存在次数 $< n$ 的多项式 $u(X), v(X)$ 使得

$fu+gv=1$; 由此得到 $g(\theta)v(\theta)=1$, 从而 $1/g(\theta)=v(\theta)$. 数 n 可以看作有基元素 $1,\theta,\cdots,\theta^{n-1}$ 的 P 上向量空间的维数.

在任意扩张 $F\supset P$ 的情形, 将 F 看作 P 上向量空间也是适宜的. 它的维数 $\dim_P F$ (可能是无限的) 我们用 $[F:P]$ 来记, 并将它叫做**扩张 F 在 P 上的次数**. 若 $F=P(\theta)$, 则 $[F:P]$ 也叫做**本原元素的次数**. 显然, 对于超越元 $\theta\in F, 1,\theta,\theta^2,\cdots$, 这一族元素在 P 上线性无关, 从而 $[P(\theta):P]=\infty$. 另一方面, 从上面所说的可以推出以下断言.

定理 1 设 F 是域 P 的任意一个扩张. 元素 $\theta\in F$ 在 P 上是代数的当且仅当 $[P(\theta):P]<\infty$. 此外, θ 的代数性导致等式 $P(\theta)=P[\theta]$.

我们称 $K\supset F\supset P$ 是**扩张的两层塔**. 它允许我们谈到三个向量空间: K/P (P 上的 K), K/F (F 上的 K) 及 F/P (P 上的 F). 它们的维数以一种关系联系起来, 这种关系和子群的指数之间的关系相类似.

定理 2 在扩张的塔$K\supset F\supset P$ 中, 次数 $[K:P]$ 是有限的当且仅当次数 $[K:F]$ 及 $[F:P]$ 都是有限的. 在它们是有限的情形, 有关系式

$$[K:P]=[K:F][F:P]$$

证明 首先假设 $[K:F]$ 及 $[F:P]$ 是有限的. 我们在 F/P 中选定 P–基 $f_1,\cdots,f_m$, 并在 K/F 中选 F–基 $e_1,\cdots,e_n$. 则任意元素 $x\in K$ 可写成 $x=\sum\limits_j \alpha_j e_j$ 这种形状, 其中 $\alpha_j\in F$. 同样, $\alpha_j=\sum\limits_i p_{ij}f_i$, 其中 $p_{ij}\in P$. 因此, $x=\sum\limits_{ij}p_{ij}f_ie_j$, 从而我们看到, mn 个元素 f_ie_j 在 P 上线性地生成 K. 假定对于某些 $p_{ij}\in P$, 存在线性相关式 $\sum\limits_{ij}p_{ij}f_ie_j=0$, 则

$$0=\sum_{i,j}p_{ij}f_ie_j=\sum_j\left(\sum_i p_{ij}f_i\right)e_j\Longrightarrow\sum_i p_{ij}f_i=0\Longrightarrow p_{ij}=0$$

对所有 $i=1,\cdots,m;j=1,\cdots,n$ 成立, 这是因为 $e_1,\cdots,e_n$ 在 F 上是线性无关的, 而 $f_1,\cdots,f_m$ 在 P 上是线性无关的. 于是 mn 个元素 f_ie_j 组成向量空间 K/P 的基, 从而 $[K:P]=nm=[K:F][F:P]$.

反之, 不等式 $[K:P]<\infty$ 导致 $[F:P]$ 的有限性, 这是因为 F/P 是空间 K/P 的子空间. 若 $(a_1,\cdots,a_r)$ 是 K 的 P–基, 则任意元素 $x\in K$ 将是 $a_1,\cdots,a_r$ 的线性组合, 其系数在 P 中, 因此, 其系数也在 F 中. 在 F 上, $a_1,\cdots,a_r$ 当中线性无关元的个数只可能更小. 因此, $[K:F]<\infty$. □

推论 设 F 是域 P 的扩张, A 是 F 中所有 P 上代数元组成的集合. 则 A 是 F 中包含 P 的子域.

证明 每一个元素 $t \in P$ 是线性多项式 $X - t \in P[X]$ 的根, 因此, $P \subset A$. 进一步, 设 $u, v \in A$. 则根据定理 1, 我们有 $[P(u) : P] < \infty$. P 上代数元 v 也将是 $P(u)$ 上代数元, 即

$$[P(u,v) : P(u)] = [P(u)(v) : P(u)] < \infty.$$

根据定理 2,

$$[P(u,v) : P] = [P(u,v) : P(u)][P(u) : P] < \infty.$$

因为 $u - v, uv \in P(u,v)$, 因此, 再根据定理 1, 我们有 $u - v, uv \in A$. 即 A 是 F 的子环. 它是域, 这是因为

$$0 \neq u \in A \Longrightarrow [P(u^{-1}) : P] = [P(u) : P] < \infty. \qquad \square$$

扩张 $F \supset P$ 叫做 P 上**代数扩张**, 如果 F 中所有元素都是 P 上代数元. 代数扩张中的每一个元素 α 是某个由 α 确定的不为零的标准多项式 (即最高次项系数为 1) $f \in P[X]$ 的根. 若 $f(\alpha) = 0$ 而对任何 $0 \neq g \in P[X]$ 且 $\deg g < \deg f$, 都有 $g(\alpha) \neq 0$, 则 $f = f_\alpha$ 叫做**元素 α 的极小多项式**. 极小多项式在 P 上是不可约的, 也是唯一确定的, 并且它的次数和元素 α 的次数一致 (对极小多项式乘上一个常数所得到的多项式常常也叫做极小多项式). 多项式 f_α 的所有不相同的根都认为是和 α **共轭的**. 下面的定理 3 将对这个术语作出解释. 若 $\mathrm{char}\, P = 0$, 则不相同的根的个数和 $\deg f_\alpha$ 一致 ([BA I], 第 6 章), 但在一般情形并非如此 (见习题 4 及 5).

根据所得到的结果, $[F : P]$ 次有限次扩张 $F \supset P$ 是**有限代数扩张**, 即它是由对 P 添加有限个代数元 $\alpha_1, \cdots, \alpha_m$ 得到的. 反之: *每一个有限代数扩张 $F = P(\alpha_1, \cdots, \alpha_m)$ 具有有限次数.* 事实上, $f_k(\alpha_k) = 0, 1 \leqslant k \leqslant m, f_k \in P[X]$. P 上代数元 α_k 自然也将是 $P(\alpha_1, \cdots, \alpha_{k-1})$ 上代数元. 这意味着 $[P(\alpha_1, \cdots, \alpha_k) : P(\alpha_1, \cdots, \alpha_{k-1})] < \infty$, 因此, 根据定理 2,

$$[F : P] = [P(\alpha_1, \cdots, \alpha_m) : P] = \prod_{k=1}^{m} [P(\alpha_1, \cdots, \alpha_k) : P(\alpha_1, \cdots, \alpha_{k-1})] < \infty. \qquad \square$$

例 域 $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ 作为 $\mathbb{Q}$ 上向量空间是四维的: $F = \langle 1, \sqrt{2}, \sqrt{3}, \sqrt{6} \rangle_{\mathbb{Q}}$, 即每一个元素 $\alpha \in F$ 可写成线性组合 $\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ 这种形状, 它具有有理坐标 a, b, c, d. 另一方面,

$$F = \langle 1, \theta, \theta^2, \theta^3 \rangle_{\mathbb{Q}}, \text{其中 } \theta = \sqrt{2} + \sqrt{3}$$

事实上,

$$\sqrt{2} = -\frac{9}{2}\theta + \frac{1}{2}\theta^3, \quad \sqrt{3} = \frac{11}{2}\theta - \frac{1}{2}\theta^3, \quad \sqrt{6} = -\frac{5}{2} + \frac{1}{2}\theta^2.$$

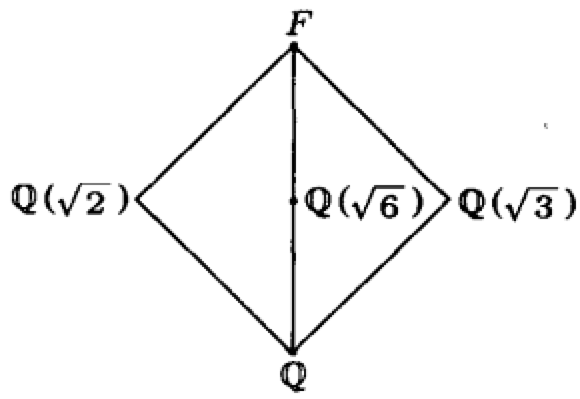
本原元素 θ 有极小多项式 $f_\theta(X) = X^4 - 10X^2 + 1$, 其根为

$$\theta^{(1)} = \theta = \sqrt{2} + \sqrt{3}, \quad \theta^{(2)} = \sqrt{2} - \sqrt{3}$$
$$\theta^{(3)} = -\sqrt{2} + \sqrt{3}, \quad \theta^{(4)} = -\sqrt{2} - \sqrt{3}$$

将注意力转向这样一个事实, 即 F 是多项式 $f_\theta(X)$ 的分裂域, 并且

$$F = \mathbb{Q}\left(\theta^{(1)}, \theta^{(2)}, \theta^{(3)}, \theta^{(4)}\right) = \mathbb{Q}\left(\theta^{(i)}\right), \quad i = 1, 2, 3, 4.$$

在伽罗瓦一般理论中, 这样的域曾被叫做是**正规的**. 域 F 的子域图



和四元群 V_4 的子群图相类似, 而这也并不是偶然的. 如果我们考察任意自同构 $\Phi: F \to F$, 则由关系式

$$\Phi(x+y) = \Phi(x) + \Phi(y), \quad \Phi(xy) = \Phi(x)\Phi(y) \quad \forall x, y \in F$$

可推出, Φ 完全由它自己在本原元素 θ 上的作用决定. 又, $\Phi(a) = a, \forall a \in \mathbb{Q}$, 因此

$$\Phi(\theta)^4 - 10\Phi(\theta)^2 + 1 = \Phi\left(\theta^4 - 10\theta^2 + 1\right) = \Phi(0) = 0.$$

这就是说, $\Phi(\theta)$ 是根 $\theta^{(i)}, i = 1, 2, 3, 4$, 当中的一个, 从而我们得到结论: 由所有自同构组成的群 $\mathrm{Aut}(F/\mathbb{Q})$ (也被称为**伽罗瓦群** $G(F/\mathbb{Q})$ 或 $G(f_\theta)$) 具有阶 $4 = [F:\mathbb{Q}]$. 4 阶群精确到同构总共只有两个: 循环群 Z_4 及 $Z_2 \times Z_2 \cong V_4$. 直接计算即可证明 $\mathrm{Aut}(F/\mathbb{Q}) \cong V_4$.

将 $\mathrm{Aut}(F/\mathbb{Q})$ 用作用在集合 $\Omega = \{1, 2, 3, 4\}$ 上的置换来表示: 用 Ω 的元素来对根 $\theta^{(i)}$ 编号, 就可以非常容易地确信这一点. 例如, 若 $\Phi\left(\theta^{(1)}\right) = \theta^{(2)}$, 则

$$\begin{aligned} \theta^{(1)}\theta^{(2)} &= -1 \Longrightarrow \theta^{(2)}\Phi\left(\theta^{(2)}\right) = -1 \\ &\Longrightarrow \Phi\left(\theta^{(2)}\right) = \theta^{(1)}, \quad \Phi\left(\theta^{(3)}\right) = -\Phi\left(\theta^{(2)}\right) = -\theta^{(1)} = \theta^{(4)}. \end{aligned}$$

即 $\Phi \approx (1\ 2)(3\ 4)$. 类似地得到自同构 $(1\ 3)(2\ 4) = \tau$ 及 $(1\ 4)(2\ 3) = \sigma\tau$.

剩下来还需补充的是循环子群 $\langle\sigma\rangle$ 使中间域 $\mathbb{Q}(\sqrt{2})$ 的元素不动, 因此 $\langle\sigma\rangle$ 是域 F 关于子域 $\mathbb{Q}(\sqrt{2})$ 的所有自同构作成的群 (伽罗瓦群) $G = \mathrm{Aut}(F/\mathbb{Q}\sqrt{2})$. 类似地, $\langle\tau\rangle$ 及 $\langle\sigma\tau\rangle$ 的不动元域相应地是 $\mathbb{Q}(\sqrt{3})$ 及 $\mathbb{Q}(\sqrt{6})$, 而伽罗瓦群 $G = \mathrm{Aut}(F/\mathbb{Q}(\sqrt{3})), G = \mathrm{Aut}(F/\mathbb{Q}(\sqrt{6}))$ 也就是 $\langle\tau\rangle$ 及 $\langle\sigma\tau\rangle$. 我们就特例检验了正规域 F 的子域和它的自同构群的子群之间的伽罗瓦一一对应的正确性.

2. 分裂域的同构 在第 4 章 §1 中曾定义并构造了标准多项式在 P 上的分裂域. 我们注意到在构造中有随意想象的元素. 现在来重复这一构造. 我们只能说 $[F:P]<n!$ (请尽力设法理解为什么). 然而事实上给定的多项式 f 在 P 上的所有分裂域都是同构的. 为了使得这一说法更加准确, 我们考察一些更一般的情况. 根据 [BA I] 第 5 章 §2 中的定理 3, 域 P 到域 $\widetilde{P}$ 的任一同构映射 φ 可以如下唯一的方式延拓为 $P[X]$ 到 $\widetilde{P}[X]$ 的同构

$$f(X)=X^n+a_1X^{n-1}+\cdots+a_n\mapsto\widetilde{f}[X]=\varphi_X f=X^n+\varphi(a_1)X^{n-1}+\cdots+\varphi(a_n).$$

定理 3 设 $\varphi:P\to\widetilde{P}$ 是域的同构; $f\in P[X]$ 是次数 $n>0$ 的标准多项式, $\widetilde{f}=\varphi_X f$ 是它的在同构 φ_X 作用下的像; $F,\widetilde{F}$ 相应地是 $f,\widetilde{f}$ 在 P 和 $\widetilde{P}$ 上的分裂域. 则 φ 可以用 $k\leqslant[F:P]$ 种方法延拓为同构 $\Phi:F\to\overline{F}$, 并且如果多项式 $f(X)$ 的所有根都不相同, 则 $k=[F:P]$.

证明 第 I 步. 首先考察任意扩张 $K\supset P$, $\widetilde{K}\supset\widetilde{P}$ 的情形. 设 $\theta\in K$ 是代数元, 其极小多项式是 $g=g_\theta\in P[X]$. 我们断言, 当且仅当 $\widetilde{g}$ 在 $\widetilde{K}$ 中有根时, 同构 $\varphi:P\to\widetilde{P}$ 可延拓为单射 $\rho:P(\theta)\to\widetilde{K}$, 并且延拓的个数和多项式 $\widetilde{g}$ 在 $\widetilde{K}$ 中不相同的根的个数一致.

事实上, 由 ρ 的存在性推出元素 $\rho(\theta)$ 应该是 $\widetilde{g}$ 的根:

$$g(\theta)=0\Longrightarrow\widetilde{g}(\rho(\theta))=\rho(g(\theta))=0.$$

反之, 若 $g(\omega)=0$, 则 $\mathrm{Ker}\psi\supset g(X)P[X]$, 其中 $\psi:P[X]\to\widetilde{K}$ 是由对应 $u(X)\mapsto\widetilde{u}(\omega)$ 确定的同态. 正如在群的情形一样, ψ 导出同态

$$\overline{\psi}:P[X]/g(X)P[X]\to\widetilde{K}$$

$(u(X)+g(X)P[X]\mapsto\widetilde{u}(\omega)$; 如果这一点并不完全清楚, 则必须重新转向第 4 章的结果). 我们注意到由于 $g(X)$ 是不可约的, 商环 $P[X]/g[X]P[X]$ 是域, 因此, $\overline{\psi}$ 是单射. 用完全同样的方法, 可以确定域的同构 $\overline{\sigma}:P[X]/g(X)P[X]\to P(\theta)$ $(u(X)+g(X)P[X]\mapsto u(\theta))$. 合成 $\rho=\overline{\psi}\circ\overline{\sigma}^{-1}$ 是 $P(\theta)$ 到 $\widetilde{K}$ 的单射 $(\rho(u(\theta))=\widetilde{u}(\omega))$. 因为 $P(\theta)$ 是元素 θ 在 P 上生成的, 所以 ρ 是 φ 的将 θ 作用成 ω 的唯一的一个延拓. 这已意味着其限制为 $\rho|_P=\varphi$ 的不相同单射 ρ 的个数等于多项式 $\widetilde{g}(X)$ 在 $\widetilde{K}$ 中不相同的根的个数.

第 II 步. 分裂域是用一连串地添加不可约多项式的根来构造的. 下面对维数 $[F:P]$ 用归纳法. 当 $[F:P]=1$ 时, 多项式 f 已在 $P[X]$ 中可分解成线性因式: $f(X)=(X-c_1)\cdots(X-c_n)$. 在这种情形, $\widetilde{f}(X)=(\varphi_X f)(X)=(X-\widetilde{c}_1)\cdots(X-\widetilde{c}_n)$. 多项式 $\widetilde{f}$ 的根 $\widetilde{c}_1,\cdots,\widetilde{c}_n$ 包含在 $\widetilde{P}$ 中, 而因为 $\widetilde{F}$ 由它们在 $\widetilde{P}$ 上生成, 所以 $\widetilde{F}=\widetilde{P}$, 因此 $\Phi=\varphi_X$ 是唯一的一个延拓.

当 $[F:P]>1$ 时, 我们在 P 上将 $f(X)$ 分解成标准不可约因式, 在这些不可约因式当中至少应该有一个多项式其次数 $m>1$. 我们将它用 $g(X)$ 来表示. 因为

$$f(X)=g(X)h(X) \Longrightarrow \widetilde{f}(X)=(\varphi_X f)(X)=\widetilde{g}(X)\widetilde{h}(X),$$

所以在分裂域 F 和 $\widetilde{F}$ 上有多项式的分解

$$g(X)=(X-\theta_1)\cdots(X-\theta_n),$$
$$\widetilde{g}(X)=(X-\omega_1)\cdots(X-\omega_m), \quad m\leqslant n.$$

由于不可约性, $g(X)$ 是元素 θ_1 在 P 上的极小多项式, 并且 $[P(\theta_1):P]=m$.

若在 $\omega_1,\cdots,\omega_m$ 当中有 l 个是不相同的, 则根据第 I 步, 存在扩张 $L=P(\theta_1)$ 到 $\widetilde{F}$ 的 l 个单射 $\rho_1,\cdots,\rho_l$, 其限制是 $\rho_i|_P=\varphi$. 分裂域的构造是这样的, 即 F 可以认为是多项式 $f\in L[X]$ 在 L 上的分裂域, 而 $\widetilde{F}$ 可以认为是多项式 $\widetilde{f}(X)$ 在 $\rho_i(L)$ 上的分裂域, 对于任何 $i=1,2,\cdots,l$. 根据定理 2 有不等式

$$[F:L]=\frac{[F:P]}{m}<[F:P].$$

因此根据归纳假定 ρ_i 当中的每一个可以延拓成同构 $\Phi_{i,j}:F\to\widetilde{F}$, 并且这种延拓的个数 (指数 j 的个数) 不超过 $[F:L]$, 而且若多项式 $\widetilde{f}$ 在 $\widetilde{F}$ 中的所有根都不相同, 则它等于这个上界. 因为

$$\Phi_{i,j}|_L=\rho_i, \quad 1\leqslant j\leqslant[F:L], \quad \rho_i|_P=\varphi,$$

所以 $\Phi_{i,j}$ 是 φ 的延拓, 并且

$$\rho_i\neq\rho_s \Longrightarrow \Phi_{i,j}\neq\Phi_{s,t} \quad \text{当 } i\neq s \text{ 时}.$$

于是, 总共得到同构 φ 的 $k\leqslant m[F:L]=[F:P]$ 个延拓. 若多项式 $\widetilde{f}$ 的根都不相同, 这个不等式就转为等式.

第 III 步. 最后, 设 $\Phi:F\to\widetilde{F}$ 是同构 φ 的任意延拓. 和第 II 步中一样, 限制 $\Phi|_L$ 作为 L 到 $\widetilde{F}$ 的单射和 ρ_i 当中的一个一致, 而在这种情形, Φ 和 $\Phi_{i,j}$ 当中的一个一致. □

推论 1 多项式 $f\in P[X]$ 在 P 上的任意两个分裂域 $F,\widetilde{F}$ 同构.

事实上, 只要在定理 3 中命 $\widetilde{P}=P$ 并取域 P 到自身的恒等映射作为 φ 即可. □

推论 2 多项式 $f\in P[X]$ 在 P 上的任意分裂域的自同构群 $\operatorname{Aut}F/P$ 是有限群, 并有阶 $\leqslant[F:P]$. 若多项式 $f(X)$ 的所有的根都不相同, 则 $|\operatorname{Aut}F/P|=[F:P]$.

证明 由定理 3 直接推出. □

注 虽然多项式 $f \in \mathbb{Q}[X]$ 在 $\mathbb{Q}$ 上 (或在任何其它数域上) 的分裂域可以认为是置入复数域 $\mathbb{C}$ 中的, 因此是唯一确定的. 但是推论 2 指出, 即使在这种情形, 将定理 3 的证明研究清楚仍是有意义的.

扩张 $\overline{P}/P$ 叫做域 P **的代数闭包**, 若它是代数扩张并且域 $\overline{P}$ 是代数闭的. 不太难证明每一个域 P 都有代数闭的扩张, 它在精确到 P–同构意义下是唯一确定的. 任一代数扩张 F/P 可以用 $\leqslant [F:P]$ 种方法嵌入到域 P 的代数闭包 $\overline{P}$ 中.

3. 本原元素的存在性 $P[X]$ 中的多项式叫做**可分的**, 如果它的不可约因式的根不相同. 域 P 叫做**完全域**, 如果每一个多项式 $f \in P[X]$ 都是可分的. 显然, 任何一个特征为零的域 P 都是完全的. 另一方面, 有

定理 4 *设 P 是特征为 $p > 0$ 的域. 则 P 是完全域当且仅当 $P = P^p$ (P 中所有元素的 p 次幂作成的集合).*

证明 若 $P^p \subsetneqq P$ 而 $a \in P \backslash P^p$, 则多项式 $X^p - a$ 不可约 (见下面的习题 4). 此外, $(X^p - a)' = pX^{p-1} = 0$, 因此 $X^p - a$ 不是可分多项式, 而这就是说, P 不是完全域.

反之, 假定 $f(X)$ 是 $P[X]$ 中不可分的不可约多项式, 即 $\text{g.c.d}(f, f') \neq 1$. 则 $f(X) = a_0 + a_pX^p + a_{2p}X^{2p} + \cdots$. 若对任何 i, 有 $a_i = b_i^p$, 则 $f(X) = (b_0 + b_1X + b_2X^2 + \cdots)^p$, 它和 $f(X)$ 的不可约性矛盾. 因此, 存在 i 使 $a_i \notin P^p$. 所以 $P^p \neq P$. □

通过对 P 添加有限多个可分元 (不可约可分多项式的根) 所得到的有限代数扩张 $F \supset P$ 叫做**可分扩张**. 如果不去考虑域 P 的代数闭包 $\overline{P}$, 则可以限于 (按定义是置于 $\mathbb{C}$ 中的) 代数数域.

定理 5 *设 F 是域 P 的有限扩张. 本原元素 $\theta \in F$ (当 $F = P(\theta)$ 时) 存在当且仅当中间域 $E\,(F \supset E \supset P)$ 的个数有限. 若 F 在 P 上可分, 则本原元素 θ 存在.*

证明 对于有限域 P 这完全是清楚的, 这是因为 $F^* = \langle\theta\rangle$, 因此 θ 是本原元素. 设 P 是无限域.

首先假定中间域的个数有限. 设 $\alpha, \beta \in F$. 命 c 走遍 P 中的元素. 根据条件我们只能得到有限多个 $P(\alpha + c\beta)$ 这种类型的域. 因此, 存在 $c_1, c_2 \in P, c_1 \neq c_2$ 使得

$$E := P(\alpha + c_1\beta) = P(\alpha + c_2\beta).$$

我们注意到

$$\alpha + c_1\beta, \alpha + c_2\beta \in E \Longrightarrow (c_1 - c_2)\beta \in E \Longrightarrow \beta \in E \Longrightarrow \alpha \in E,$$

即 $P(\alpha, \beta) = E = P(\alpha + c_1\beta)$. 用归纳法, 我们得到结论: 若 $F = P(\alpha_1, \cdots, \alpha_n)$, 则存在 $c_2, \cdots, c_n \in P$ 使

$$F = P(\theta), \quad \theta = \alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n.$$

这证明了第一个断言的一半.

反之, 假定对于某个 θ 有 $F = P(\theta)$, 且 $f = f_\theta(X)$ 是 θ 的极小多项式. 设 $P \subset E \subset F$, 并设 $g_{E,\theta}$ 是 θ 在 E 上的极小多项式. 显然, $g_{E,\theta}$ 整除 f_θ. 但 $F[X]$ 是唯一因子分解整环; $F[X]$ 中整除 $f(X)$ 的任意标准多项式等于若干个因子 $X - \alpha_i$ 的乘积, 其中 $\alpha_1, \cdots, \alpha_n$ 是 f 的根. 因此, 只有有限多个这种多项式. 我们得到从中间域的集合到多项式的有限集的一个映射 $E \mapsto g_E$.

设 E_0 是 E 的由 $g_E(X)$ 的系数在 P 上生成的子域. 则 g_E 的系数在 E_0 中, 并且在 E_0 上不可约, 这是因为它在 E 上不可约. 因此, 元素 θ 在 E_0 上的次数和 θ 在 E 上的次数一致, 而这给出等式 $E = E_0$. 所以我们的域 E 由和它联系起来的多项式 g_E 唯一确定. 因此, 映射 $E \mapsto g_E$ 是单射. 这完成了定理的第一个断言的证明.

至于说到关于可分扩张的断言, 则我们用归纳法, 并且不失一般性, 我们可以假定 $F = P(\alpha, \beta)$, 其中 α, β 在 P 上可分. 设 $\varphi_1, \cdots, \varphi_n$ 是 $P(\alpha, \beta)$ 在域的代数闭包 $\overline{P}$ 中不相同的嵌入. 命

$$f(X) = \prod_{i \neq j} (\varphi_i\alpha + X\varphi_i\beta - \varphi_j\alpha - X\varphi_j\beta).$$

则 $f(X) \neq 0$. 因此, 存在 $c \in P$ 使 $f(c) \neq 0$. 元素 $\varphi_i(\alpha + c\beta)$ 当 $i = 1, 2, \cdots, n$ 时是不相同的, 由此推得 $[P(\alpha + c\beta) : P] \geqslant n$. 但 $[P(\alpha, \beta) : P] = n$, 因此

$$P(\alpha, \beta) = P(\alpha + c\beta).$$

换句话说, $\theta = \alpha + c\beta$ 是本原元素. □

习 题

1. 证明: 素数次扩张 $F \supset P$ 没有真 $(\neq P, F)$ 子域.
2. 求扩张 $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}\right)$ 的本原元素, 其中 p 和 q 是素数.
3. 求多项式 $X^p - 2$ 的分裂域在 $\mathbb{Q}$ 上的维数.
4. 证明: 在特征为 $p > 0$ 的域 P 上, 对于多项式 $X^p - a$ 来说只有两种可能: 是不可约的或是一个线性多项式的 p 次幂.
5. 设 $Z_p(Y)$ 是特征为 p 的有理分式域. 证明: $X^p - Y$ 是 $Z_p(Y)$ 上不可约多项式, 其所有根都相同.

§2 有限域

1. 存在性和唯一性 除了 $Z_p = \mathbb{Z}/p\mathbb{Z}$ 以外, 我们还遇到过有限域的其它例子. 到了将它们纳入一般理论的时候了. 最先的观察是关于有限域的任意有限扩张.

命题 1　设 F 是元素个数为 q 的域, 并且 $K \supset F$ 是次数为 $[K:F]=n$ 的扩张, 则 $|K|=q^n$.

证明　事实上, 当选定基以后, F 上向量空间 K 和长度为 n 的行 $(\alpha_1,\cdots,\alpha_n)$ 的空间 F^n 等同. 所有的坐标 α_i 互相独立地取 F 中 q 个值. 这就是说, $|K|=|F^n|=q^n$. □

命题 2　任意有限域 F 具有有限特征 p (p 是素数) 且 $|F|$ 是 p 的幂.

证明　事实上, 由于 F 的有限性, 素子域应该同构于域 $Z_p=\mathbb{Z}/p\mathbb{Z}$. 根据命题 1, $|P|=p$ 的有限扩张 $F\supset P$ 具有势 $|F|=p^m$. □

定理 1　对于每一个有限域 F 及对于每一个正整数 n, 存在一个且精确到同构时只有一个扩张 $K\supset F$, 其次数是 $[K:F]=n$.

证明　**唯一性**　设 $K\supset F$ 是 n 次扩张. 根据命题 2, $|F|=q \Longrightarrow q=p^m, p$ 是素数, 并且 $|K|=q^n$. 因此, 乘法群 $K^*=K\backslash\{0\}$ 具有阶 q^n-1, 而其每一个元素的阶根据拉格朗日定理整除 $q^n-1: t^{q^n-1}=1, \forall t\neq 0$. 这就是说域 K 的所有元素 (包括 $t=0$ 在内) 是多项式 $X^{q^n}-X$ 的不相同的根并且有分解

$$X^{q^n}-X=\prod_{t\in K}(X-t).$$

在 K 的任何一个元素个数 $<q^n$ 的真子域上, 都不可能有这种分解成线性因式的分解, 因此 K 是多项式 $X^{q^n}-X$ 的分裂域. 转向 §1 中定理 3 的推论 1, 我们得到所要求的结论.

存在性　在证明唯一性时所作的论述提示了构造 K 的可能途径. 取多项式 $f(X)=X^{q^n}-X$ 在 $P\cong Z_p$ 上的分裂域作为 K. 因为 $q=p^m$, 所以在 K 中 $q\cdot 1=0$. 因此 $f'(X)=q^n\cdot 1\cdot X^{q^n-1}-1=-1$. 所以根据已知的判别法 ([BA I] 第 6 章 §1, 定理 4), $f(X)$ 没有重根. 这就是说, 多项式 $f(X)$ 的根作成的子集 $K_f\subset K$ 具有势 $|K_f|=q^n$.

因为 $K_f\subset K$ 且 $\operatorname{char} K=p$, 所以根据 [BA I] 第 4 章 §3 习题 6, $(x+y)^{p^s}=x^{p^s}+y^{p^s}$ 对任何 $x,y\in K_f$ 及 $s=0,1,2,\cdots$ 成立 (注意到 $F\subset K_f$). 特别地,

$$x,y\in K_f \Longrightarrow (x\pm y)^{q^n}=x^{q^n}\pm y^{q^n}=x\pm y \Longrightarrow x\pm y\in K_f.$$

此外,

$$1\in K_f;\quad (xy)^{q^n}=x^{q^n}y^{q^n}=xy\Longrightarrow xy\in K_f;$$
$$0\neq x\in K_f \Longrightarrow (x^{-1})^{q^n}=x^{-1}\Longrightarrow x^{-1}\in K_f.$$

因此, K_f 是 K 的包含 F 及多项式 $f(X)$ 的所有根的子域. 根据分裂域的定义, 应该有等式 $K_f=K$. 次数 $[K:F]=n$, 这是因为 $q^{[K:F]}=|K|=|K_f|=q^n$. □

推论 对于每一个素数 p 及对于每一个正整数 n, 存在一个且当精确到同构时只有一个域, 其元素个数是 p^n.

证明包含在将定理 1 应用于特殊情形 $|F| = p$ 之中. □

2. 有限域的子域及自同构. 正如我们在 [BA I] 第 4 章 §3 中已经注意到, 元素个数为 $q = p^n$ 的有限域通常用符号 $\mathbb{F}_q$ 来记, 或者, 为了记念 E. 伽罗瓦, 用符号 $GF(p^n)$ 来记. 我们确立有限域的一系列性质.

定理 2 以下断言成立.

i) 有限域 $\mathbb{F}_q$ 的乘法群 $\mathbb{F}_q^*$ 是 $q-1$ 阶循环群.

ii) 元素个数为 $q = p^n$ 的有限域 $\mathbb{F}_q$ 的自同构群 $\mathrm{Aut}\,\mathbb{F}_q$ 是 n 阶循环群, 且

$$\mathrm{Aut}\,\mathbb{F}_q = \langle \Phi | \Phi(t) = t^p, \forall t \in \mathbb{F}_q \rangle.$$

iii) 若 $\mathbb{F}_{p^d}$ 是域 $\mathbb{F}_{p^n}$ 的子域, 则 $d|n$. 反之: 对于数 n 的每一个因子 d, 相应地正好有一个子域 $\{t \in \mathbb{F}_{p^n} | \Phi^d(t) = t\} = \mathbb{F}_{p^d}$. 使这个子域的元素保持不动的自同构组成一个群 $\mathrm{Aut}(\mathbb{F}_{p^n}|\mathbb{F}_{p^d}) = \langle \Phi^d \rangle$. 因此, 在有限域 $\mathbb{F}_q$ 的子域和它的自同构群的子群之间有一个双射 (伽罗瓦对应).

iv) 若 $q = p^n$, 且 $\mathbb{F}_q^* = \langle \theta \rangle$, 则 θ 是域的有 n 次极小多项式 $h(X)$ 的本原元素, 且 $\mathbb{F}_q$ 是多项式 $h(X)$ 在 $\mathbb{F}_p$ 上的分裂域.

v) 对于任意自然数 m, 至少存在一个 $\mathbb{F}_q$ 上 m 次不可约多项式.

证明 i) 见第 2 章 §3 中的定理 11.

ii) 我们将把 $\mathbb{F}_q$ 看作是其素子域 $\mathbb{F}_p \cong Z_p$ 的 n 次有限扩张. 因为 $\mathbb{F}_q$ 是所有的根都不相同的多项式 $X^q - X$ 的分裂域, 所以, 根据 §1 中定理 3 的推论 2, $|\mathrm{Aut}\mathbb{F}_q| = n$. 在定理 1 的证明过程中已经注意到 $(x+y)^p = x^p + y^p, (xy)^p = x^p y^p, 1^p = 1$. 根据这个关系, 明显可知, $\Phi : t \mapsto t^p$ 是域 $\mathbb{F}_q$ 的自同构 ($\mathbb{F}_q$ 的有限性是非常重要的). 若 $\Phi^s : t \mapsto t^{p^s}$ 是恒等自同构, 则对于所有 $t \in \mathbb{F}_q$, 有 $t^{p^s} - t = 0$, 由此推出不等式 $s \geqslant n$. 然而当 $s = n$ 时, 我们真的得到恒等自同构, 因此 $|\langle \Phi \rangle| = n$ 且 $\langle \Phi \rangle = \mathrm{Aut}\mathbb{F}_q$.

iii) 根据命题 1, $p^n = (p^d)^r$, 其中 r 是扩张 $\mathbb{F}_{p^n} \supset \mathbb{F}_{p^d}$ 的次数. 因此, $n = dr$. 反之, 对于任何 $d|n$, 我们引入子集 $F = \{t \in \mathbb{F}_{p^n} | t^{p^d} = t\}$. 因为 $n = dr \Longrightarrow p^n - 1 = (p^d)^r - 1 = (p^d - 1)k$, 所以

$$X^{p^n-1} - 1 = X^{(p^d-1)k} - 1 = \left(X^{p^d-1} - 1\right) g(X),$$
$$X^{p^n} - X = \left(X^{p^d} - X\right) g(X).$$

因为 $\mathbb{F}_{p^n}$ 是多项式 $X^{p^n} - X$ 的分裂域, 所以 $\mathbb{F}_{p^n}$ 中正好有 p^d 个元素是 $X^{p^d} - X$ 的根. 这些元素恰好组成子集 F, 它现在可以和 $\mathbb{F}_{p^d}$ 等同. 用这一与定理 1 对偶的论证也确立了有 p^d 个元素的子域的唯一性.

我们注意到, 根据构造,

$$\mathbb{F}_{p^d} = \left\{t \in \mathbb{F}_{p^n} | \Phi^d(t) = t\right\}$$

是在 $\langle\Phi^d\rangle$ 作用下所有不动元组成的集合. 因为群 $\mathrm{Aut}\,(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle\Phi\rangle$ 是循环群, 所以直接看出, 任何不属于 $\langle\Phi^d\rangle$ 的自同构作用在 $\mathbb{F}_{p^d}$ 上时都不是恒同的 (只要将 Φ^l 应用于群 $\mathbb{F}_{p^d}^*$ 的生成元即可). 这也就是说, 相应的自同构群 $\mathrm{Aut}\,(\mathbb{F}_{p^n}/\mathbb{F}_{p^d})$ 和 $\langle\Phi^d\rangle$ 一致. 断言 iii) 中的结论性词句和第 1 目中的例子中的结论性词句有同样的意义.

iv) 完全明显, $\mathbb{F}_q = \mathbb{F}_p(\theta), q = p^n$, 设 $h(X) = X^n + a_1X^{n-1} + \cdots + a_n$ 是本原元素 θ 的极小多项式. 因为素子域 $\mathbb{F}_p$ 的元素在所有自同构作用下都不动, 而 $a_i \in \mathbb{F}_p$, 所以, $\theta, \theta^p, \theta^{p^2}, \cdots, \theta^{p^{n-1}}$ 是 $h(X)$ 的根. 它们全都包含在我们的域中, 从而

$$\mathbb{F}_p\left(\theta, \cdots, \theta^{p^{n-1}}\right) = \mathbb{F}_p(\theta) = \mathbb{F}_{p^n}$$

是多项式 $h(X)$ 在 $\mathbb{F}_p$ 上的分裂域.

v) 根据定理 1, 我们来构造 m 次扩张 $K \supset \mathbb{F}_q$. 根据 i), K^* 是循环群. 若 $K^* = \langle\theta\rangle$ 且 $h(X)$ 是本原元素 θ 的极小多项式, 则 $K = \mathbb{F}_q(\theta)$ 且 $\deg h(X) = [\mathbb{F}_q(\theta) : \mathbb{F}_q] = [K : \mathbb{F}_q] = m$. 根据定义, 极小多项式是不可约的 (在 $\mathbb{F}_q$ 上), 因此我们得到了所需要的. □

在不复杂的数论准备以后, 我们将得到 $\mathbb{F}_q$ 上 m 次不可约多项式的个数的精确公式.

3. 默比乌斯 (Möbius) 反演公式及其应用 由规则

$$\mu(n) = \begin{cases} 1, & \text{若 } n = 1, \\ (-1)^k, & \text{若 } n = p_1 \cdots p_k, \quad p_i \text{ 是不相同的素数}, \\ 0, & \text{若 } n \text{ 被 } > 1 \text{ 的平方整除}. \end{cases}$$

定义的数论函数 μ 叫做**默比乌斯函数**. 很清楚, 在 μ 不恒等于零且对任何互素的 m 及 n 均有 $\mu(mn) = \mu(m)\mu(n)$ 的意义下, μ 是**乘性函数**. 同样显然, 若 $n = p_1^{m_1} \cdots p_r^{m_r}$, 则

$$\sum_{d|n} \mu(d) = \sum_{d|n_0} \mu(d),$$

其中 $n_0 = p_1 \cdots p_r$ 是数 n 的不含平方的极大因子. 对于固定的 s, 数 n_0 的因子 $d = p_{i_1} \cdots p_{i_s}$ 的个数等于 $\begin{pmatrix} r \\ s \end{pmatrix}$. 因此, 当 $n > 1$ 时, 我们有

$$\sum_{d|n} \mu(d) = \sum_{d|n_0} \mu(d) = \sum_{s=0}^{r} \begin{pmatrix} r \\ s \end{pmatrix} (-1)^s = (1-1)^r = 0.$$

(左端求和是对整数 n 的所有因子 $d \geqslant 1$ 进行的). 最后得到公式

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{若 } n = 1, \\ 0, & \text{若 } n > 1. \end{cases} \tag{1}$$

它的变形

$$\sum_{d|n|m} \mu\left(\frac{m}{n}\right) = \begin{cases} 1, & \text{若 } d = m, \\ 0, & \text{若 } d|m, \quad d < m \end{cases} \tag{2}$$

也是有用的 (求和是对整除 m 而又被 d 整除的 n 进行的). 命 $m = dt, n = dl$, 并命 l 走遍数 t 的因子, 我们容易从 (2) 转到 (1) 以及反过来.

公式 (1) (或 (2)) 可以取作默比乌斯函数的归纳定义. 它对我们的价值包含在下面的断言中.

设 f 及 g 是从 $\mathbb{N}$ 到 M 的任意两个函数 (M 等于 $\mathbb{Z}, \mathbb{R}, F[X]$ 等等), 它们由关系式

$$f(n) = \sum_{d|n} g(d) \tag{3}$$

联系起来, 则

$$g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d) \tag{4}$$

事实上, 注意到 (2), 将 (3) 的两边同乘 $\mu(m/n)$ 后直接对整除 m 的 n 求和即给出

$$\sum_{n|m} \mu\left(\frac{m}{n}\right) f(n) = \sum_{n|m} \mu\left(\frac{m}{n}\right) \sum_{d|n} g(d) = \sum_{d|m} g(d) \sum_{d|n|m} \mu\left(\frac{m}{n}\right) = g(m).$$

简单地更换一下符号就导致公式 (4), 它叫做**默比乌斯反演公式**. 以类似的方式可以完成由 (4) 到 (3) 的转变. □

还有默比乌斯反演公式的乘性类似物: 若 $f(n) = \prod_{d|n} g(d)$, 则

$$g(n) = \prod_{d|n} f(d)^{\mu(n/d)} \tag{5}$$

为了证明, 必须进行一些形式计算:

$$\begin{aligned} \prod_{n|m} f(n)^{\mu(m/n)} &= \prod_{n|m} \prod_{d|n} g(d)^{\mu(m/n)} = \prod_{d|m} \prod_{d|n|m} g(d)^{\mu(m/n)} \\ &= \prod_{d|m} g(d)^{\sum_{d|n|m} \mu(m/n)} = g(m), \end{aligned}$$

然后稍微地改变一下符号.

我们举出默比乌斯反演公式的应用的三个例子.

1) **欧拉函数** φ. 根据定义, $\varphi(n)$ 是一串数 $1,2,\cdots,n-1$ 中和 n 互素的数的个数, 或等于说, $\varphi(n)=|U(Z_n)|$ 是环 $Z_n=\mathbb{Z}/n\mathbb{Z}$ 的可逆元群的阶. 从第 3 章 §1 的习题 5 我们知道有关系式

$$n=\sum_{d|n}\varphi(d) \tag{6}$$

根据公式 (4) 直接得到

$$\varphi(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)d=\sum_{d|n}\mu(d)\frac{n}{d}=n\sum_{d|n}\frac{\mu(d)}{d}.$$

若 $n=p_1^{m_1}\cdots p_r^{m_r}$, 则

$$\begin{aligned}\sum_{d|n}\frac{\mu(d)}{d}&=1-\sum_i\frac{1}{p_i}+\sum_{i<j}\frac{1}{p_ip_j}-\cdots+(-1)^r\frac{1}{p_1p_2\cdots p_r}\\&=\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right).\end{aligned}$$

因此,

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$$

是我们在 [BA I] 中就已经得到过的公式, 并且由它直接导出函数 φ 的乘性性质.

2) **分圆多项式.** 多项式 X^n-1 在 $\mathbb{Q}$ 上的分裂域 Γ_n 叫做**分圆域**. 因为 1 的所有 n 次根组成 n 阶循环群, 所以分圆域具有形状 $\Gamma_n=\mathbb{Q}(\zeta)$, 其中 ζ 是本原根当中的一个 $(\zeta\in\mathbb{C})$. 我们希望求出次数 $[\Gamma_n:\mathbb{Q}]$ 及元素 ζ 在 $\mathbb{Q}$ 上的极小多项式.

用符号 P_n 表示 1 的 n 次本原根组成的集合, 其势 $|P_n|=\varphi(n)$. n 阶循环群的子群和数 n 的因子 d 之间有一个双射对应, 而每一个根 ζ^i 落入某个集合 P_d. 因此, 有分成不相交的类的一个划分,

$$\{1,\zeta,\zeta^2,\cdots,\zeta^{n-1}\}=\bigcup_{d|n}P_d \tag{7}$$

(转向集合的势, 我们重新又得到关系式 (6)). $\varphi(n)$ 次多项式

$$\Phi_n(X)=\prod_{\zeta}(X-\zeta)$$

叫做相应于 Γ_n 的**分圆多项式**. 相应于划分 (7), 我们得到分解式

$$X^n-1=\prod_{i=0}^{n-1}(X-\zeta^i)=\prod_{d|n}\left\{\prod_{\zeta\in P_d}(X-\zeta)\right\}=\prod_{d|n}\Phi_d(X). \tag{8}$$

将默比乌斯乘性反演公式应用于 (8), 得到 Φ_n 的明显表示式:

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)} \tag{9}$$

对于 n 的不大的值, 我们有

$$\Phi_1(X) = X - 1, \quad \Phi_2(X) = X + 1, \quad \Phi_3(X) = X^2 + X + 1,$$
$$\Phi_4(X) = X^2 + 1, \quad \Phi_6(X) = X^2 - X + 1, \quad \Phi_8(X) = X^4 + 1,$$
$$\Phi_9(X) = X^6 + X^3 + 1, \quad \Phi_{10}(X) = X^4 - X^3 + X^2 - X + 1,$$
$$\Phi_{12}(X) = X^4 - X^2 + 1.$$

我们看到

$$\Phi_n(X) \in \mathbb{Z}[X], \quad \Phi_n(0) = 1, \quad n > 1. \tag{10}$$

为了得到 (10), 可以不通过 (9), 采用归纳法. 对于不大的 n, 这已被检验过. 接下去, 我们以下面的方法来论证. 我们认为

$$g(X) = \prod_{d|n, d\neq n} \Phi_d(X)$$

是整系数标准多项式, 并应用带余除法 (见 [BA I]), 我们得到唯一确定的多项式 $q, r \in \mathbb{Z}[X]$ 使得

$$X^n - 1 = q(X)g(X) + r(X), \quad \deg r(X) < \deg g(X).$$

但在 $\mathbb{Q}[X]$ 中, $X^n - 1 = \Phi_n(X)g(X)$, 我们看到, $\Phi_n(X) = q(X) \in \mathbb{Z}[X]$, 并且 $g(X)$ 的标准性质导致 $\Phi_n[X]$ 的标准性质.

在 [BA I] 中已经确立了多项式

$$\Phi_p(X) = (X^p - 1)/(X - 1) = X^{p-1} + X^{p-2} + \cdots + 1$$

的不可约性, 其中 p 是任意素数. 关于对任何 $n, \Phi_n(X)$ 的不可约性问题我们留到下一节中去讨论.

3) **$\mathbb{F}_q$ 上不可约的多项式.** 设 $\Psi_d(q)$ 是 $\mathbb{F}_q$ 上 d 次不可约标准多项式的总个数, $q = p^n$, 并设 $f(X)$ 是这些多项式当中的一个. 它在 $\mathbb{F}_q$ 上的分裂域既同构于商环 $\mathbb{F}_q[X]/(f(X))$, 又同构于多项式 $X^{q^d} - X$ 的分裂域 (定理 1 的推论). 由于 $f(X)$ 的不可约性, 多项式 $X^{q^d} - X$ 和 $f(X)$ 存在公共根 θ 就导致 $X^{q^d} - X$ 被 $f(X)$ 整除. 因为对任何 $m = rd$, $X^{q^d} - X$ 是多项式 $X^{q^m} - X$ 的因子, 并且因为 $X^{q^d} - X$ 没有重根, 所以我们得到结论: 对于任何 $d|m$, $X^{q^m} - X$ 在 $\mathbb{F}_q$ 上的分解式中, 所有 d 次最高次项系数为 1 的不可约多项式

$$f_{d,1}, f_{d,2}, \cdots, f_{d,\Psi_d(q)}(X)$$

都出现在其中, 且每一个都恰好出现一次:

$$X^{q^m} - X = \prod_{d|m} \left\{ \prod_{k=1}^{\Psi_d(q)} f_{d,k}(X) \right\}. \tag{11}$$

计算等式 (11) 两边的多项式的次数, 就导致关系式

$$q^m = \sum_{d|m} d\Psi_m(q),$$

由此, 直接应用默比乌斯反演公式 (4) 就得到 $\Psi_m(q)$ 的表达式:

$$\Psi_m(q) = \frac{1}{m} \sum_{d|m} \mu\left(\frac{m}{d}\right) q^d. \tag{12}$$

例如, 设 $q = 2$, 则

$$\begin{aligned} &\Psi_2(2) = \frac{1}{2}(2^2 - 2) = 1, \quad \Psi_3(2) = \frac{1}{3}(2^3 - 2) = 2, \\ &\Psi_4(2) = \frac{1}{4}(2^4 - 2^2) = 3, \quad \Psi_5(2) = \frac{1}{5}(2^5 - 2) = 6, \\ &\Psi_6(2) = \frac{1}{6}(2^6 - 2^3 - 2^2 + 2) = 9. \end{aligned}$$

公式 (12) 指出, 随机取出的 $\mathbb{F}_q$ 上 m 次标准多项式为不可约多项式的概率接近于 $1/m$. 然而对于具体地取出的多项式并没有令人满意的不可约性判别法. 例如, 关于三项式 $X^m + X^k + 1$ 的不可约性能说些什么? 这类问题在代数编码论中及伪随机序列的构造中经常发生.

习 题

1. 证明对于任何 $d|n, d < n$, 有关系式 $X^n - 1 = (X^d - 1)\Phi_n(X)h_d(X)$, 其中 $h_d \in \mathbb{Z}[X]$.

2. 设 q 是 > 1 的正整数. 根据 (10), $\Phi_n(q) \in \mathbb{Z}$. 证明: $\Phi_n(q)|(q-1) \Longrightarrow n = 1$.

3. 验证: 分圆多项式

$$\Phi_{15}(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$$

当作域 $\mathbb{F}_2$ 上多项式时是两个不可约多项式 $X^4 + X^3 + 1$ 及 $X^4 + X + 1$ 的积. 利用这种情况, 证明 $\Phi_{15}(X)$ 在 $\mathbb{Q}$ 上的不可约性 (和 [BA I] 第 6 章 §1 中的习题 11 作比较).

4. 验证分圆多项式的以下性质:

若 p 是素数且 $p|n$, 则 $\Phi_{pn}(X) = \Phi_n(X^p)$; 而若 $p \nmid n$, 则 $\Phi_{pn}(X) = \Phi_n(X^p)/\Phi_n(X)$.

5. 从自然包含链

$$GF(p) \subset GF\left(p^{2!}\right) \subset GF\left(p^{3!}\right) \subset \cdots$$

出发, 引入所谓极限域 $\Omega_p = GF\left(p^{\infty!}\right)$, 其中

$$\alpha \in \Omega_p \Longleftrightarrow \left\{\alpha \in GF\left(p^{n!}\right) \text{ 对于充分大的 } n\right\}.$$

根据有限域的基本性质, 证明 Ω_p 是代数闭域. 因此, 考虑到复数域 $\mathbb{C}$, 得到任意特征的代数闭域的例子.

6. 设 $q = p^n$. 证明: 当 $p = 2$ 时, 域 $\mathbb{F}_q$ 的所有元素都是平方, 而当 $p > 2$ 时, 群 $\mathbb{F}_q^*$ 中的平方在其中组成指数为 2 的子群 $\mathbb{F}_q^{*2}$, 并且 $\mathbb{F}_q^{*2} = \operatorname{Ker}\left(t \mapsto t^{(q-1)/2}\right)$.

7. (阿希巴谢尔 (M. Aschbacher)). 设 $\mathbb{F}_q$ 是有限域, 其元素个数是奇数 $q = p^n$. 若 q 不等于 3 或 5, 则 "在圆周" $x^2 + y^2 = 1$ 上存在具有坐标 $x, y \in \mathbb{F}_q^*$ 的点. 对于 $p > 5$ 证明这个断言.

8. 是否域 $\mathbb{F}_q$ 的每一个本原元素都是乘法群 $\mathbb{F}_q^*$ 的生成元?

9. 设 $A(q) = \mathrm{Ass}_F(X_1, \cdots, X_q)$ 是域 F 上自由结合代数, 它由 q 个自由生成元 (非交换的变元 $X_1, \cdots, X_q$) 生成. 命

$$\mathrm{A_m}(q) = \langle X_{i_1} X_{i_2} \cdots X_{i_m} \,|\, 1 \leqslant i_j \leqslant q \rangle_F, \quad \dim A_m(q) = q^m,$$

我们看到 $A(q)$ 是分次代数

$$A(q) = F \cdot 1 \oplus A_1(q) \oplus A_2(q) \oplus A_3(q) \oplus \cdots$$

在 $A(q)$ 中包含自由李代数 $L(q) = \mathrm{Lie}(X_1, \cdots, X_q)$, 它有同样的自由生成元并有换位运算 $[UV] = UV - VU$. 代数 $L(q)$ 也是分次的:

$$L(q) = L_1(q) \oplus L_2(q) \oplus L_3(q) \oplus \cdots,$$

其中

$$L_1(q) = \langle X_1, \cdots, X_q \rangle_F, \quad L_2(q) = \langle [X_i, X_j] | \, i < j \rangle_F, \cdots$$

利用雅可比恒等式, 我们确信

$$L_3(q) = [[X_i, X_j], X_k], \quad i < j, k \leqslant j, \quad \dim L_3(q) = \frac{1}{3}\left(q^3 - q\right).$$

事实上, 有广义维特 (Witt) 公式

$$\dim L_m(q) = \Psi_m(q) = \frac{1}{m} \sum_{d|m} \mu\left(\frac{m}{d}\right) q^d, \tag{12'}$$

它十分准确地和公式 (12) 一致. 本质差别只在于 (12′) 中的 q 是任意自然数, 而 (12) 中的 q 是素数的幂.

第 3 章开头问题 2 中的项链数也可用此公式表达.

§3 伽罗瓦对应

1. 初步结果　设 $F \supset P$ 是 P 上某个不可约多项式 $f(X)$ 的分裂域, $\operatorname{Aut} F/P$ 是域 F 的所有使 $\eta(a) = a, \forall a \in P$ 的自同构 η 组成的集合. 正如我们从 §1 知道的, $|\operatorname{Aut} F/P| \leqslant [F : P]$, 并且如果多项式 f 的所有根都不相同, 则 $|\operatorname{Aut} F/P| = [F : P]$.

定义　群 $\operatorname{Aut} F/P$ 通常叫做扩张 F/P 的**伽罗瓦群**, 并记作 $\operatorname{Gal} F/P$. 这个术语已在包括 §1 在内的一系列地方用过.

以后域 P 将假定是完全的, 因此,

$$|\operatorname{Gal} F/P| = [F : P].$$

设 $H \subset \operatorname{Gal} F/P$ 是伽罗瓦群的任意子群. 命

$$F^H = \{a \in F | \varphi(a) = a \ \forall \varphi \in H\}.$$

因此, $\mathbb{F}^H$ 是 F 中所有在 H 的作用下保持不动的元素作成的子域. 有两个映射:

1) $H \mapsto K = F^H$ 是从子群 $H \subset \operatorname{Gal} F/P$ 的集合到子域 $F \supset K \supset P$ 的集合的映射;

2) $K \mapsto H = \operatorname{Gal} F/K$ 是从中间子域 $F \supset K \supset P$ 的集合到子群 $H \subset \operatorname{Gal} F/P$ 的集合的映射.

有明显的性质:

i) $G = \operatorname{Gal} F/P \supset G_1 \supset G_2 \Longrightarrow F^{G_1} \subset F^{G_2}$;

ii) $F \supset P_1 \supset P_2 \supseteq P \Longrightarrow \operatorname{Gal} F/P_1 \subset \operatorname{Gal} F/P_2$;

iii) $F^{\operatorname{Gal} F/P} \supset P$;

iv) $\operatorname{Gal} F/F^H \supset H$ 对任何子群 $H \subset G$.

我们将暂时把 $K \supset P$ 理解成域 P 的任意扩张 (不一定是分裂域).

引理 (E. 阿廷)　设 G 是域 K 的有限自同构群且 $P = K^G$. 则

$$[K : P] \leqslant |G|.$$

证明　命 $n = |G|$. 我们必须证明 K 中任意 $m > n$ 个元素在 P 上是线性相关的. 设

$$G = \{\varphi_1 = e, \varphi_2, \cdots, \varphi_n\}, \quad u_1, u_2, \cdots, u_m \in K, \quad m > n.$$

由 m 个未知量 $x_1, x_2, \cdots, x_m, n$ 个线性方程构成的齐次线性方程组

$$\sum_{j=1}^{m} \varphi_i(u_j) x_j = 0, \quad 1 \leqslant i \leqslant n$$

有非平凡解 $(a_1, \cdots, a_m) \neq (0, \cdots, 0)$. 在所有解中取 $(b_1, \cdots, b_m)$ 其非零分量个数是最小的. 不失一般性可以认为 $b_1 \neq 0$, 甚至认为 $b_1 = 1$. 只要证明 $b_j \in K^G$, $\forall j$, 这是因为相应于 $\varphi_1 = e$ 的第一个关系式将有形状 $\sum\limits_{j=1}^{m} u_j b_j = 0$.

假定对某个 j, 有 $b_j \notin P$. 在可能的改变记法以后, 我们认为 $b_j = b_2$. 将 φ_k 应用于方程组, 其中 k 取成使 $\varphi_k(b_2) \neq b_2$. 我们得到

$$\sum_j (\varphi_k \varphi_i)(u_j) \varphi_k(b_j) = 0, \quad 1 \leqslant i \leqslant n,$$

或者同样地,

$$\sum_j \varphi_i(u_j) \varphi_k(b_j) = 0, \quad 1 \leqslant i \leqslant n.$$

这是因为对于固定的 k, $\varphi_k \varphi_i (i = 1, \cdots, n)$ 走遍群 G 的所有元素. 因此, $(1, \varphi_k(b_2), \cdots, \varphi_k(b_m))$ 也是方程组的解. 从 $(1, b_2, \cdots, b_m)$ 中减去它, 我们得到解

$$(0, b_2 - \varphi_k(b_2), \cdots, b_m - \varphi_k(b_m)),$$

它也是非平凡的, 这是因为由于 φ_k 的取法, 有 $b_2 - \varphi_k(b_2) \neq 0$. 然而它的非零分量的个数比 $(b_1, b_2, \cdots, b_m)$ 的非零分量的个数小, 这与后者的选取相违. □

定义 扩张 F/P 叫做**正规代数扩张**, 如果每一个在 F 中至少有一个根的不可约多项式 $f \in P[X]$ 在 $F[X]$ 中是线性因子的乘积. 换句话说, F 包含每一个元素 $a \in F$ 的极小多项式 f_a 的分裂域.

根据定义, "正规性加可分性" 这一性质等价于 $P[X]$ 中每一个在 F 中有根的不可约多项式是 $F[X]$ 中不相同的线性因子的乘积. 正规可分代数扩张 $F \supset P$ 也叫做**伽罗瓦扩张**. 若 F 是多项式 $f \in P[X]$ 的分裂域, 则 $\mathrm{Gal}\, F/P$ 也叫做多项式 $f(X)$ (或方程 $f(X) = 0$) 在 P 上的**伽罗瓦群**, 并记作 $\mathrm{Gal}(f)$.

定理 1 扩张 F/P 上的下列条件是等价的:

1) F 是某个可分多项式 $f(X)$ 在 P 上的分裂域;

2) 对于某个有限群 $G \subseteq \mathrm{Aut}\, F$, $P = F^G$;

3) F 是 P 的有限维正规可分扩张.

断言 1) 和 2) 下面的补充也成立:

补充 1). 若 F 及 P 和在 1) 中一样, 且 $G = \mathrm{Gal}\, F/P$, 则 $P = F^G$;

补充 2). 若 F 及 P 和在 2) 中一样, 则 $G = \mathrm{Gal}\, F/P$.

证明 1)$\Longrightarrow$2). 在 1) 中命 $G = \mathrm{Gal}\, F/P$ 且 $P' = F^G$. 则 P' 是 F 中包含 P 的子域. 也很清楚, F 是多项式 $f(X)$ 在 P' 上的分裂域, 并且 $G = \mathrm{Gal}\, F/P'$.

由于 f 的可分性, 我们有 $|G| = [F : P']$, 就像 $|G| = [F : P]$ 一样. 但 $F \supset P' \supseteq P \Longrightarrow [F : P] = [F : P'][P' : P] \Longrightarrow [P' : P] = 1 \Longrightarrow P' = P$. 而这就是 2). 我们也证明了对于 $G = \mathrm{Gal}\, F/P$ 有 $P = F^G$, 即补充 1).

2)$\Longrightarrow$3). 根据阿廷引理,

$$P = F^G \Longrightarrow [F : P] \leqslant |G|,$$

因此, F 在 P 上是有限维的. 设 f 是 $P[X]$ 中有根 $r \in F$ 的不可约多项式. 我们将认为

$$\{r_1 = r, r_2, \cdots, r_m\} = \{\varphi(r) | \varphi \in G\}$$

是有代表 r 的 G–轨道. 若 $\psi \in G$, 则 $\{\psi(r_1), \cdots, \psi(r_m)\}$ 是根 $r_1, \cdots, r_m$ 的一个重新排序. 当然, $f(r) = 0 \Longrightarrow f(r_i) = 0$. 这就是说, $f(X)$ 被 $X - r_i$ 整除, 而由于 $r_i (1 \leqslant i \leqslant m)$ 是不相同的, 因此 $f(X)$ 被 $g(X) = \prod_{i=1}^{m} (X - r_i)$ 整除.

将环 $F[X]$ 的自同构 $X \mapsto X, a \mapsto \psi(a), a \in F$ 应用于 $g(X)$, 则

$$\psi \cdot g(X) = \prod_{i=1}^{m} (X - \psi(r_i)) = \prod_{i=1}^{m} (X - r_i) = g(X),$$

于是我们看到多项式 $g(X)$ 的系数是 G–不变的. 因此 $g(X) \in P[X]$, 这是由于 $F^G = P$. 但 f 被假定是在 P 上不可约的, 这就是说,

$$f(X) = g(X) = \prod_{i=1}^{m} (X - r_i)$$

是 $F[X]$ 中不相同线性因子的乘积, 即扩张 F 在 P 上是可分的和正规的, 这就断定了 3).

3)$\Longrightarrow$1). 因为 $[F : P] < \infty$, 所以 $F = P(r_1, \cdots, r_k)$, 其中 r_i 是 P 上代数元. 设 $f_i(X)$ 是 r_i 在 P 上的极小多项式. 根据条件, $f_i(X)$ 是 $F[X]$ 中不相同线性因子的乘积. 由此推出, $f(X) = \prod f_i(X)$ 是可分的, 而 F 是 $f(X)$ 在 P 上的分裂域, 因此, 我们得到 1).

还需证明补充 2). 我们已看到, 在条件 2) 中根据阿廷引理 $[F : P] \leqslant |G|$, 而根据刚才才证明过的, 条件 3) 成立, 因此 $|\mathrm{Gal}\, F/P| = [F : P]$. 因为 $F^G = P \Longrightarrow G \subset \mathrm{Gal}\, F/P$ 且 $|G| \geqslant [F : P] = |\mathrm{Gal}\, F/P|$, 所以 $G = \mathrm{Gal}\, F/P$. □

2. 基本的伽罗瓦对应　现在我们已经准备好去证明核心的断言.

定理 2　设 F 是域 P 的满足定理 1 中任何一个条件的扩张. 设 $G = \mathrm{Gal}\, F/P$ 是伽罗瓦群, $\Gamma = \{H\}$ 是 G 的子群的集合且 $\sum$ 是 F 和 P 之间的中间域的集合. 则映射

$$\begin{cases} H \mapsto F^H, \\ K \mapsto \mathrm{Gal}\, F/K \end{cases}$$

是 Γ 到 $\sum$ 及 $\sum$ 到 Γ 的双射. 此外, 这个伽罗瓦对应具有以下性质:

i) $H_1 \supset H_2 \iff F^{H_1} \subset F^{H_2}$;

ii) $|H| = [F : F^H], (G : H) = [F^H : P]$;

iii) $H \lhd G \iff F^H$ 在 P 上是正规的. 在后一情形,

$$\mathrm{Gal}\,(F^H/P) \cong G/H.$$

证明 设 $G = \mathrm{Gal}\,F/P, H \in \Gamma$. 因为 $P = F^G$, 所以 $P \subset F^H$ 且 $K = F^H$ 是 F 中包含 P 的子域. 这给出映射 $\Gamma \to \sum$. 应用定理 1, 补充 2) 并用 H 代替 G, 我们看到 $\mathrm{Gal}\,F/F^H = H$, 由此推出断言 ii) 的第一个部分: $|H| = |\mathrm{Gal}\,F/F^H| = [F : F^H]$.

现在设 K 是 F 和 P 之间的任一子域. 命 $H = \mathrm{Gal}\,F/K$. 则 $H \subset G = \mathrm{Gal}\,F/P$, 因此 H 是 G 的子群. 同样也很清楚, F 是某个可分多项式在 K 上的分裂域, 这是因为它是 P 上这种域. 于是, 将定理 1, 补充 1) 应用于 F 及 K, 就得到 $K = F^H$. 我们证实了在定理的表述中用 "{" 指出的映射是双射.

在本节开始即已看出一个明显性质, 即若 $H_1 \supset H_2$, 则 $F^{H_1} \subset F^{H_2}$. 反之, 若 $F^{H_1} \subset F^{H_2}$, 则 $H_1 = \mathrm{Gal}\,F/F^{H_1} \supset \mathrm{Gal}\,F/F^{H_2} = H_2$, 这给出了 i).

性质 ii) 的第一个部分早已看到了. 因为

$$|G| = [F : P] = [F : F^H][F^H : P] = [H][F^H : P]$$

及 $|G| = |H|[G : H]$, 所以明显有 $[F^H : P] = [G : H]$, 而这证明了性质 ii) 的第二个部分.

最后, 我们来确立性质 iii) 的正确性. 若 $H \in \Gamma$ 且 $K = F^{H'}$ 是对应的子域, 则对应于共轭子群 $\psi H \psi^{-1}$ 的子域 K' 是 $\psi(K)$ (为了明显起见, G 中作共轭化的元素用希腊字母来记). 这一点立即可以看出, 这是因为条件 $\varphi(x) = x, \forall x \in K$ 等价于 $(\psi\varphi\psi^{-1})\psi(x) = \psi(x)$, 即 $\psi(x) \in K'$. 由此推出

$$H \lhd G \iff \psi(K) = K = F^H, \quad \forall \psi \in G.$$

假定对每一个元素 $\psi \in G$, 有 $\psi(K) = K$. 在这种情形, 限制 $\overline{\psi} = \psi|_K$ 是域 K 在 P 上的自同构, 从而我们得到群 $G = \mathrm{Gal}\,F/P$ 到 $\mathrm{Gal}\,K/P$ 的同态 $\psi \to \overline{\psi}$, 其像 $\overline{G}$ 是 K 的自同构群, 且明显有 $F^{\overline{G}} = P$, 于是 $\overline{G} = \mathrm{Gal}\,K/P$.

同态 $\psi \to \overline{\psi}$ 的核是使得 $\psi|_K = 1_K$ 的这种元素 $\psi \in G$ 组成的集合. 伽罗瓦对应说明, 这个集合就是 $\mathrm{Gal}\,F/K = H$. 因此 $\overline{G} = \mathrm{Gal}\,K/P \cong G/H$.

因为 $P = F^{\overline{G}}$, 所以根据定理 1,3), K 在 P 上是正规的. 反之, 假定域 K 在 P 上是正规的, 我们考察任意元素 $a \in K$ 在 P 上的极小多项式 f_a. 则在 $K[X]$ 中, $f(X) = (X - a_1)(X - a_2) \cdots (X - a_m)$, 其中 $a_1 = a$. 若 $\varphi \in G$, 则 $f_a(\varphi(a)) = 0$, 由此推出对某个 $i, \varphi(a) = a_i$. 因此, $\varphi(a) \in K$, 从而 $\varphi(K) \subset K$. 和以前一样, 这意味着, 对于在伽罗瓦对应中和 K 对应的每一个子群 H 都有 $\varphi H \varphi^{-1} \subset H$. 这就是说, $H \lhd G$. 这完成了 iii) 的证明. □

3. 伽罗瓦对应的例证 在开始两节中考察过的域 $\mathbb{Q}(\sqrt{2},\sqrt{3})$ 以及有限域 $\mathbb{F}_q$ 是伽罗瓦理论的序幕. 我们来扩充例证材料.

A) **分圆域** Γ_n. 我们来考察和 $\varphi(n)$ 次分圆多项式 $\Phi_n(X)$ (见 §2) 相联系的正规扩张 $\Gamma_n=\mathbb{Q}(\zeta),\zeta^n=1$, 其 $\Phi_n(X)$ 的根是且仅是 1 的全部 n 次本原根. 我们首先来证明

定理 3 分圆多项式 $\Phi_n(X)$ 在 $\mathbb{Q}$ 上不可约, 因此 $[\Gamma_n:\mathbb{Q}]=\varphi(n)$.

证明 正如我们已经知道的, $\Phi_n(X)\in\mathbb{Z}[X]$. 根据高斯引理, 在 $\mathbb{Q}[X]$ 上的不可约性等价于在 $\mathbb{Z}[X]$ 上的不可约性. 假定

$$\Phi_n(X)=g(X)h(X),$$

其中 $g,h\in\mathbb{Z}[X]$, 并且次数 $\geqslant 1$ 的多项式 $h(X)$ 在 $\mathbb{Z}[X]$ 中 (从而也在 $\mathbb{Q}[X]$ 中) 不可约. 设 p 是不整除 n 的素数且 $h(\lambda)=0$. 因为 $\text{g.c.d}\,(p,n)=1$, 所以 λ^p 是 1 的 n 次本原根.

若 $h(\lambda^p)\neq 0$. 则 $g(\lambda^p)=0$. 于是 λ 是多项式 $g(X^p)$ 和 $h(X)$ 的根. 由于 h 的不可约性, 我们有 $h(X)|g(X^p)$, 即

$$g(X^p)=h(X)l(X),\quad l\in\mathbb{Z}[X].$$

我们有

$$X^n-1=\Phi_n(X)d(X)=d(X)g(X)h(X).$$

转向模 p 的同余式, 即我们将在 $\mathbb{Z}_p[X]$ 中进行:

$$X^n-\bar{1}=\bar{d}(X)\bar{g}(X)\bar{h}(X) \tag{$*$}$$

$(f(X)=a_0X^m+a_1X^{m-1}+\cdots\in\mathbb{Z}[X]\Longrightarrow\bar{f}(X)=\bar{a}_0X^m+\bar{a}_1X^{m-1}+\cdots\in\mathbb{F}_p[X])$

类似地, $\bar{g}(X^p)=\bar{h}(X)\bar{l}[X]$. 但是对于任意 $f\in\mathbb{Z}[X]$, 我们有

$$\bar{f}(X)^p=\bar{a}_0X^{pm}+\bar{a}_1X^{p(m-1)}+\cdots=\bar{f}(X^p).$$

因此 $\bar{g}(X)^p=\bar{g}(X^p)=\bar{h}(X)\bar{l}[X]$, 当然由此推出 $\text{g.c.d}\,(\bar{g},\bar{h})\neq 1$.

根据 $(*)$, 我们得到结论: $X^n-\bar{1}$ 在它自己在 $\mathbb{Z}_p$ 上的分裂域中有重根. 但这不可能, 这是因为 $(X^n-\bar{1})'=\bar{n}X^{n-1}$ 且 $\bar{n}\neq 0$. 因此, $\text{g.c.d}\left(X^n-\bar{1},(X^n-\bar{1})'\right)=\bar{1}$. 所得到的矛盾表明: $h(\lambda)=0\Longrightarrow h(\lambda^p)=0$, 对每一个素数 $p\nmid n$. 重复这一论证就得知, 对于与 n 互素的任意自然数 r, λ^r 是多项式 $h(X)$ 的根. 但是 1 的每一个 n 次本原根具有形状 λ^r, $\text{g.c.d}\,(r,n)=1$. 于是 $h(X)$ 被 $X-\lambda'$ 整除, 其中 λ' 是任意 n 次本原根. 在这种情形 $h(X)=\Phi_n(X)$, 即 Φ_n 不可约. □

设 $G = \mathrm{Gal}\,\Gamma_n/\mathbb{Q}$. 则 $\sigma \in G \Longrightarrow \sigma(\zeta) = \zeta^m$, 对某个整数 $m = \widetilde{m}(\sigma)$, 并且 $\mathrm{g.c.d}\,(\widetilde{m}(\sigma), n) = 1$, 以及 $(\sigma(\zeta))^n = 1$. 又

$$\sigma, \tau \in G \Longrightarrow (\sigma\tau)(\zeta) = \zeta^{\widetilde{m}(\sigma\tau)} = \sigma\left(\zeta^{\widetilde{m}(\tau)}\right) = \zeta^{\widetilde{m}(\sigma)\widetilde{m}(\tau)},$$

即 $\widetilde{m}(\sigma\tau) = \widetilde{m}(\sigma)\widetilde{m}(\tau)$, 因此 $\widetilde{m} : G \to U(Z_n)$ 是域 Γ_n 的伽罗瓦群到模 n 与 n 互素的整数作成的乘法群 $U(Z_n)$ 的同态. 这个同态是单射, 这是因为 $\widetilde{m}(\sigma)$ 的指数由自同构 σ 模 n 唯一确定, 而 σ 在 $\mathbb{Q}(\zeta)$ 上的作用由在 ζ 上的作用确定. 因为根据定理 3, $[\Gamma_n : \mathbb{Q}] = \varphi(n) = |U(Z_n)|$, 所以 $G \cong U(Z_n)$.

我们证明了

定理 4 *分圆域 Γ_n 有同构于 $U(Z_n)$ 的交换伽罗瓦群.*

如果用任意的一个域 P 来替代 $\mathbb{Q}$, 则一般说来只有嵌入 $G \hookrightarrow U(Z_n)$ 而不是同构. 群 $U(Z_n)$ 的结构在第 4 章中已被研究过. 我们补充指出, G 的子群是正规的. 因此, Γ_n 的每一个子域也都是正规的.

例 1 分圆域 $\Gamma_{17} = \mathbb{Q}(\zeta), \zeta^{17} = 1$ (其伽罗瓦群 $G = \mathrm{Gal}\,\Gamma_{17}/\mathbb{Q} = \langle \Phi | \Phi^{16} = 1 \rangle$ 是由映射 $\Phi : \zeta \mapsto \zeta^3$ 生成的循环群) 对于构造性数域 ([BA I] 第 5 章 § 1) 有直接关系. 我们选出下面的一串子群:

$$G = G_1 = \langle \Phi \rangle \supset G_2 = \langle \Phi^2 \rangle \supset G_3 = \langle \Phi^4 \rangle \supset G_4 = \langle \Phi^8 \rangle \supset G_5 = 1.$$

根据定理 2, 伽罗瓦对应导出子域的升链

$$\mathbb{Q} = F_1 \subset F_2 \subset F_3 \subset F_4 \subset F_5 = F = \mathbb{Q}(\zeta),$$

其中 $F_i = F^{G_i}$. 根据定义, $\Phi(\zeta) = \zeta^3, \Phi^i(\zeta) = \zeta^{3^i}$. 命 $z_1 = \sum_{i=1}^{8} \Phi^{2i}(\zeta)$, 则 $\Phi^2(z_1) = z_1, \Phi(z_1) \neq z_1$, 即 $z_1 \in F_2, z_1 \notin F_1$. 因为 $(G : G_2) = 2$, 所以 $[F_2 : F_1] = 2$, 且 $F_2 = F_1(z_1)$. 类似地, $z_2 = \sum_{i=1}^{4} \Phi^{4i}(\zeta), z_3 = \sum_{i=1}^{2} \Phi^{8i}(\zeta) = \zeta^{-1} + \zeta, F_3 = F_2(z_2), F_4 = F_3(z_3)$.

如果找到了复数 z_1, z_2, z_3 相应地在 F_1, F_2, F_3 上的极小多项式, 并用二次方程的根将这些数表达出来, 则很清楚, 它们是构造性的. 而在这种情形, 数 ζ 也是构造性的, 它给出了用直尺和圆规画出正十七边形的可能性.

关于构造性数域, 我们再作一些注解. 如果从给定的域

$$P = \mathbb{Q}(z_1, \overline{z}_1, \cdots, z_m, \overline{z}_m)$$

出发, 其中 $z_1, z_2, \cdots, z_m \in \mathbb{C}$, 则复数 z 的 P-构造性表明

$$z \in F = P(u_1, \cdots, u_r), \quad u_i^2 \in P(u_1, \cdots, u_{i-1}), \quad 1 \leqslant i \leqslant r \tag{1}$$

P 上二次扩张的塔 (1) 明显有次数 $[F:P]=2^s, s\leqslant r$. 因此, 当 $[\mathbb{Q}(\lambda):\mathbb{Q}]$ 被奇素数整除时, 复数 λ 不可能是构造性的.

B) **正 n 边形**. 当 $n=p$ 是素数时, 构造正 p 边形等于构造复数 $\zeta=\cos 2\pi/p+i\sin 2\pi/p, \zeta^{p-1}+\zeta^{p-2}+\cdots+1=0, [\mathbb{Q}(\zeta):\mathbb{Q}]=p-1$. 因此, 必要条件归结为对某个自然数 s 的等式 $p-1=2^s$. 正如在 [BA I] 第 1 章中看到的, 这种费马素数暂时只知道总共有 5 个: $3, 5, 17, 257, 65537$.

从 §2 中引入的表示式 $[\Gamma_n:\mathbb{Q}]=\varphi(n)$ 明显看出, $\varphi(n)=2^s$ 当且仅当数 n 的所有奇素因子都是费马素数并且它们在分解式中出现的重复都是 1. 这也是用圆规和直尺作正 n 边形的必要条件. 这一条件也是充分的. 但是关于这个问题, 我们就在这里停住.

C) **角的三等分**. 是否每一个角都可以用圆规和直尺分成三个相等的部分? 已经断定甚至对于 60° 的角也不可能做到, 即, 从点 $z_1=0, z_2=1, z_3=\cos 60^\circ+i\sin 60^\circ=1/2+i\sqrt{3}/2$ 出发, 点 $z=(\cos 20^\circ, \sin 20^\circ)$ 不可能被画出. 换句话说, 应该确信, 将 $\cos 20^\circ$ 添加到域 $\mathbb{Q}(\sqrt{-3})=\mathbb{Q}(z_1,z_2,z_3,\overline{z}_1,\overline{z}_2,\overline{z}_3)$ (而这是 $\mathbb{Q}$ 上 2 次扩张) 将使 $\mathbb{Q}$ 上的扩张次数 $\neq 2^s$.

事实上, 命 $u=\cos 20^\circ$ 后, 对于 $\varphi=20^\circ$, 将三角恒等式 $\cos 3\varphi=4\cos^3\varphi-3\cos\varphi$ 改写成 $4u^3-3u-1/2=0$ 或者同样地改写成 $(2u)^3-3(2u)-1=0$. 但多项式 X^3-3X-1 在 $\mathbb{Q}$ 上不可约, 因此 $[\mathbb{Q}(u):\mathbb{Q}]=3$. 而这证明了所要求的断言.

D) **倍立方.** 问题说的是构造体积为 2 的立方体的边, 即数 $\sqrt[3]{2}$ 的可构造性. 立即得到否定的回答, 这是因为多项式 X^3-2 在 $\mathbb{Q}$ 上不可约, 因此, $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$.

在 C)—D) 中, 所谈论的已不是伽罗瓦群, 而是扩张的次数. 我们举两个例子, 其中可以不太复杂地求出伽罗瓦群.

例 2 设 P 是特征为 $p>0$ 的非完全域, $a\in P\backslash P^p$. 则正如我们知道的, X^p-a 是 P 上不可约多项式. 若 $F=P(u), u^p=a$, 则 $[F:P]=p$. 此外, $X^p-a=(X-u)^p$, 即 F 是不可分多项式 X^p-a 在 P 上的分裂域. 对于 $\sigma\in \operatorname{Gal} F/P$, 我们有 $(\sigma(u))^p=a$, 因此 $\sigma(u)=u$. 这就是说 $\sigma=1$, 从而 $\operatorname{Gal} F/P$ 是单位元群.

例 3 设 $F=P(t)$, 其中 t 是 P 上超越元. 可以证明

$$F=P(u)\Longleftrightarrow u=\frac{at+b}{ct+d},\quad a,b,c,d\in P, ad-bc\neq 0.$$

映射 $\sigma:\dfrac{f(t)}{g(t)}\mapsto\dfrac{f(u)}{g(u)}$ 是伽罗瓦群 $G=\operatorname{Gal} F/P$ 的最一般形状下的元素, 因此, $G\cong \mathrm{PGL}(2,P)$.

习 题

1. 设 P 是特征为 0 的域, p 是素数, ζ 是 1 的 p 次本原根. 证明: 在域 P 中没有根的多项式

$X^p - a \in P[X]$ 在 $P[\zeta]$ 上不可约.

2. 求下列多项式的伽罗瓦群:

a) $X^3 - 12X + 8$;

b) $X^3 - 2X - 2$;

c) $X^3 + X + 1$;

d) $X^4 + 4X^2 + 2$;

e) $X^4 + 3X^3 - 3X + 3$.

§4 伽罗瓦群的计算

1. 群 Gal(f) 在多项式 f 的根上的作用 伽罗瓦群可以和根的置换群等同起来. 设 $f \in P[X]$ 是次数 $\geqslant 1$ 的多项式且它在分裂域 $F = P(\theta_1, \cdots, \theta_n)$ 中有不相同的根 $\theta_1, \cdots, \theta_n$. 最初 E. 伽罗瓦仅仅是考察了多项式 f (或方程 $f(X)=0$) 的群 $\mathrm{Gal}(f)$: 他将每一个自同构解释成对称群 S_n 的元素. 只是在很久以后, 理想理论的创立者戴德金 (R. Dedekind) 发现, $\mathrm{Gal}(f)$ 和伽罗瓦群 $\mathrm{Gal}\, F/P$ 等同. 现在已经有了在电子计算机上计算次数不大的不可约多项式 $f \in \mathbb{Z}[X]$ 的伽罗瓦群的编好了的一套程序 (Maple-V 型).

一般说来, $\mathrm{Gal}(f)$ 是 S_n 的真子群. 首先, 我们来探讨下面的问题: $F \supset P$ 中什么样的子域对应于子群 $\mathrm{Gal}(f) \subset A_n$? 其中 A_n 是交错群.

定理 1 *设 P 是特征 $\neq 2$ 的域, f 是 $P[X]$ 中次数为正数的标准多项式, 且它在分裂域 $F \supset P$ 中的根 θ_i 都不相同. 设*

$$\Delta(f) = \prod_{i<j} (\theta_i - \theta_j)$$

则 F 中对应于 $\mathrm{Gal}(f) \cap A_n$ 的子域是 $P(\Delta(f))$.

证明 设 $\pi \in S_n$. 首先我们考察环 $P[X_1, \cdots, X_n]$. 它的使 P 中每一个元素都不动的自同构 $\Phi_\pi : X_i \mapsto X_{\pi(i)}$ 可以延拓成商域 $P(X_1, \cdots, X_n)$ 的自同构, 也用 Φ_π 表示. 易知, 所有这种自同构作成的群和 S_n 同构. 利用伽罗瓦对应, 不难看出, $F^G = P(\mathrm{s}_1, \cdots, \mathrm{s}_k)$, 其中 s_k 是 $X_1, \cdots, X_n$ 的初等对称函数. 正好, $\mathrm{Gal}\, P(X_1, \cdots, X_n)/ P(\mathrm{s}_1, \cdots, \mathrm{s}_n) \cong S_n$.

命 $\Delta_n = \prod\limits_{i<j} (X_i - X_j)$. 已知并容易验证, $\Phi_\pi(\Delta_n) = \varepsilon_\pi \Delta_n$. 若 $\psi : X_i \mapsto \theta_i$ 是 $P[X_1, \cdots, X_n]$ 到 F 的同态, 则 $\psi(\Phi_\pi(\Delta_n)) = \pi(\Delta(f)) = \pm\Delta(f)$, 现在其中的 $\pi \in \mathrm{Gal}(f) \cap S_n$.

因此, 在 $\mathrm{Gal}(f) \cong \mathrm{Gal}\, F/P$ 中使子域 $P(\Delta(f)) \subset F$ 的元素不动的子群是偶置换作成的子群. 根据伽罗瓦对应, F/P 中与 $\mathrm{Gal}(f) \cap A_n$ 对应的子域将是 $P(\Delta(f)) = F^{\mathrm{Gal}(f) \cap A_n}$. □

从证明中明显看出, 对任何置换 $\pi \in \mathrm{Gal}(f)$, 都有 $\pi(\Delta(f)) = \pm\Delta(f)$. 因此, 多项式 f 的判别式 $D(f) = \Delta(f)^2$ 在 π 的作用下不动, 于是 $D(f) \in P$. 根据定理 1, 包含关系 $\mathrm{Gal}(f) \subset A_n$ 成立当且仅当 $P(\Delta(f)) = P$, 即 $\Delta(f) \in P$. 于是有

推论　设 $f \in P[X]$ 是次数 $n \geqslant 1$ 的标准多项式, $D(f) = \prod\limits_{i<j}(\theta_i - \theta_j)^2$ 是它的判别式. 则

$$\mathrm{Gal}(f) \subset A_n \Longleftrightarrow D(f) \text{ 是 } P \text{ 中元素的平方}.$$

定理 2 (不可约性判别法)　设多项式 $f \in P[X]$ 的根 $\theta_i (i = 1, \cdots, n)$ 全部都不相同. 则 f 在 P 上的不可约性等价于 $\mathrm{Gal}(f)$ 在 $\{\theta_1, \cdots, \theta_n\}$ 上作用的传递性.

证明　传递性的定义见第 1 章. 假定 f 不可约. 由 §1 中的定理 3 推出对无论怎样的 $i \neq j$, 存在同构 $P(\theta_i)/P \to P(\theta_j)/P$. 因为 $F = P(\theta_1, \cdots, \theta_n)$ 既是多项式 $f(X) = \prod\limits_k (X - \theta_k)$ 在 $P(\theta_i)$ 上, 也是在 $P(\theta_j)$ 上的分裂域, 所以根据分裂域的构造, 这一同构可以被延拓成扩张 $F \supset P$ 的自同构 σ. 这就是说, $\sigma \in \mathrm{Gal}\, F/P = \mathrm{Gal}(f)$ 且 $\sigma(\theta_i) = \theta_j$, 即 $\mathrm{Gal}(f)$ 是传递的.

反之, 假定 $\mathrm{Gal}(f)$ 在根上的作用是传递的. 设在分解式 $f(X) = g(X)h(X)$ 中, $g(X)$ 是次数为正数的不可约因式. 若对某个 i 有 $g(\theta_i) = 0$, 而 θ_j 是多项式 f 的任意一个别的根且对某个 $\sigma \in \mathrm{Gal}(f)$ 有 $\sigma(\theta_i) = \theta_j$, 则 $g(\theta_i) = 0 \Longrightarrow 0 = \sigma(g(\theta_i)) = g(\theta_j)$. 这证明了多项式 f 的每一个根都是它的因式 g 的根, 因此 $f = g$ 不可约. □

例 1　正如在 [BA I] 第 5 章 §2 中所指出的, 不完全三次方程 $f(x) = x^3 + ax + b = 0$ 的判别式是 $D(f) = -4a^3 - 27b^2$. 设 f 在基域 $\mathbb{Q}$ 中没有根, 即 f 是不可约的也是可分的. 多项式 $f_1(X) = X^3 - X - 1$ 及 $f_2(X) = X^3 - 3X + 1$ 就是这样的多项式, 它们的判别式是 $D(f_1) = -23, D(f_2) = 81 = 9^2$. 由定理 1,2 推出 $\mathrm{Gal}(f_1) \cong S_3$, 而 $\mathrm{Gal}(f_2) \cong A_3$.

例 2　$\mathbb{Q}$ 上不可约多项式 $f(X) = X^3 - 2$ 有实根 $\alpha = \sqrt[3]{2}$. 然而它的分裂域将是

$$F = \mathbb{Q}(\alpha, \varepsilon) = \langle 1, \alpha, \alpha^2, \varepsilon, \varepsilon\alpha, \varepsilon\alpha^2 \rangle_{\mathbb{Q}} = \mathbb{Q}(\theta),$$

这里

$$\varepsilon^2 + \varepsilon + 1 = 0, \quad \theta = \alpha + \varepsilon, \quad g(\theta) = 0, \quad g(X) = X^6 + 3X^5 + 6X^4 + 3X^3 + 9X + 9.$$

伽罗瓦群的结构相当明显:

$$G = \mathrm{Gal}\, F/\mathbb{Q} = \langle \sigma, \tau | \sigma^3 = e = \tau^2, \tau\sigma\tau = \sigma^2 \rangle \cong S_3,$$

其中

$$\sigma(\varepsilon) = \varepsilon, \quad \sigma(\alpha) = \varepsilon\alpha, \quad \sigma(\varepsilon\alpha) = \varepsilon^2\alpha, \quad \tau(\alpha) = \alpha, \tau(\varepsilon) = \varepsilon^2.$$

在每一个子群 $H \subseteq G$ 的下面, 我们全部写出在伽罗瓦对应下和它对应的不动元子域:

G	$\langle\sigma\rangle$	$\langle\tau\rangle$	$\langle\sigma\tau\rangle$	$\langle\sigma^2\tau\rangle$	$\{e\}$
$\mathbb{Q}$	$\mathbb{Q}(\varepsilon)$	$\mathbb{Q}(\alpha)$	$\mathbb{Q}(\varepsilon^2\alpha)$	$\mathbb{Q}(\varepsilon\alpha)$	F

于是 $\langle\sigma\rangle = \mathrm{Gal}\, F/\mathbb{Q}(\varepsilon), \langle\tau\rangle = \mathrm{Gal}\, F/\mathbb{Q}(\alpha), \langle\sigma\tau\rangle = \mathrm{Gal}\, F/\mathbb{Q}(\varepsilon^2\alpha), \langle\sigma^2\tau\rangle = \mathrm{Gal}\, F/\mathbb{Q}(\varepsilon\alpha)$. 因为 $\langle\sigma\rangle \lhd G$, 所以 $\mathbb{Q}(\varepsilon)$ 在 $\mathbb{Q}$ 上正规且 $\mathrm{Gal}\mathbb{Q}(\varepsilon)/\mathbb{Q} \cong G/\langle\sigma\rangle \cong Z_2$.

2. 素数次多项式及素数次群 具体的多项式 $f \in P[X]$ 的伽罗瓦群的计算一般是一件相当困难的事情, 甚至 $P = \mathbb{Q}$ 时也是如此. 它吸引了众多数学家的注意. 我们注意到 I. 舒尔的两个结果 (1931 年):

$$f(X) = \sum_{m=0}^{n} X^m/m! \Longrightarrow \mathrm{Gal}(f) = \begin{cases} A_n, & \text{若 } n \equiv 0 (\mathrm{mod}\, 4); \\ S_n, & \text{若 } n \not\equiv 0 (\mathrm{mod}\, 4). \end{cases}$$

设 $H_n(X)$ 是第 n 个埃尔米特多项式 (见 [BA II]). 命 $H_{2n}(X) = K_n^{(0)}(X^2)$, $H_{2n+1}(X) = XK_n^{(1)}(X^2)$, 则当 $n > 12$ 时, 有同构 $\mathrm{Gal}(K_n^{(j)}(X)) \cong S_n, j = 0, 1$. 基域是 $\mathbb{Q}$.

以后, 对称群将不止一次地出现, 因此我们引入和它们有关的两个简单的断言, 它们发展了 [BA I] 第 4 章 §3 中的习题 10.

命题 1 含有一个对换和一个长度为 $n-1$ 的循环置换的 n 次可迁置换群是对称群.

证明 设 $(1\ 2\ \cdots\ n-1)$ 是给定的 $n-1$ 循环置换. 由于群是可迁的, 对换 $(i\,j)$ 可以变成 $(k\,n)$, 其中 k 是符号 1 到 $n-1$ 中的一个. 用循环置换 $(1\ 2\ \cdots\ n-1)$ 及其幂来共轭 $(k\,n)$ 就得到对换 $(1\ n), (2\ n), \cdots, (n-1, n)$, 而它们生成了 S_n. □

命题 2 设 p 是素数. 若 $G \subseteq S_p$, 且 G 含有 p 阶元素及一个对换, 则 $G = S_p$.

证明 根据条件, G 含有 p–循环置换 $\sigma = (i_1 i_2 \cdots i_p)$, 其中 $\{i_1, i_2, \cdots, i_p\} = \{1, 2, \cdots, p\}$. 经过适当地排序后, 我们认为 $(1\,2) \in G$. 因为对某个 s 有 $\sigma^s = (1\,2 \cdots p)$, 所以认为一开始时就是 $\sigma = (1\ 2 \cdots p)$, $(1\ 2) \in G$. 那么 G 含有 $\sigma(1\ 2)\sigma^{-1} = (2\ 3)$, $\sigma(2\ 3)\sigma^{-1} = (3\ 4), \cdots, \sigma(p-2, p-1)\sigma^{-1} = (p-1, p)$. 然而 $\langle(1\ 2), (2\ 3), \cdots, (p-1, p)\rangle = S_p$. □

定理 3 设 f 是 $\mathbb{Q}$ 上素数 p 次不可约多项式. 假定 f 在 $\mathbb{C}$ 中恰好有两个非实的根, 则 $\mathrm{Gal}(f) = S_p$.

证明 命

$$f(X) = \prod_{i=1}^{p} (X - \theta_i), \quad F = \mathbb{Q}(\theta_1, \cdots, \theta_p) \subset \mathbb{C}.$$

因为

$$F \supset \mathbb{Q}(\theta_1), \quad [\mathbb{Q}(\theta_1) : \mathbb{Q}] = \deg f = p,$$

所以次数 $|\mathrm{Gal}(f)|=[F:\mathbb{Q}]$ 被 p 整除. 根据西罗定理 (见第 2 章 §2), $\mathrm{Gal}(f)$ 含有 p 阶元素. 域 $\mathbb{C}$ 的共轭自同构 $z\mapsto\overline{z}$ 延拓到 $\mathbb{C}[X]$ 后将 f 变成自己, 因此, 它对多项式 f 的根 θ_i 作了一个置换.

设 θ_1,θ_2 是非实的根, 则根据定理的条件, $\theta_2=\overline{\theta}_1$, 且当 $i>2$ 时, $\overline{\theta}_i=\theta_i$. 我们得到结论: 共轭自同构在 F 上的限制是 $\mathrm{Gal}(f)$ 中的元素, 因此就是对换. 于是 $\mathrm{Gal}(f)$ 含有 p 阶元素和对换. 剩下的只要应用命题 2. □

定理 4 (布饶尔 (R. Brauer)) *对于任何素数 p, 可以构造随便多少个其伽罗瓦群是 S_p 的 p 次不可约多项式.*

证明 设 $m;n_1,\cdots,n_{k-2}$ 是偶数, m 是正数, $n_1<n_2<\cdots<n_{k-2}$, 而 $k>3$ 是奇数. 考察有实根 $n_1,n_2,\cdots,n_{k-2}$ 的多项式

$$g(X)=\left(X^2+m\right)(X-n_1)(X-n_2)\cdots(X-n_{k-2}).$$

$y=g(x)$ 的图像有 $(k-3)/2$ 个相对极大值, 而因为对于任意奇数 h 有 $|g(h)|>2$, 所以很清楚, 这些相对极大值都 >2. 这意味着 $y=f(x)=g(x)-2$ 的图像在 n_1 和 n_{k-2} 之间有 $(k-3)/2$ 个正的相对极大值. 因此, $f(X)$ 在区间 (n_1,n_{k-2}) 中有 $k-3$ 个实根. 因为 $f(n_{k-2})=-2$ 且对任何 $M>0$, 当自然数 N 充分大时有 $f(N)>M$, 所以也存在实根 $>n_{k-2}$. 我们得到多项式 $f(X)$ 的 $k-2$ 个实根. 若

$$f(X)=\prod_{i=1}^{k}(X-\theta_i)=\left(X^2+m\right)(X-n_1)\cdots(X-n_{k-2})-2,$$

则比较系数, 将有

$$\sum_{i=1}^{k}\theta_i=\sum_{l=1}^{k-2}n_l,\quad \sum_{i<j}\theta_i\theta_j=\sum_{l<q}n_in_q+m.$$

因此,

$$\sum_i\theta_i^2=\left(\sum_i\theta_i\right)^2-2\sum_{i<j}\theta_i\theta_j=\sum_l n_l^2-2m.$$

若取 m 充分大, 则 $\sum\limits_i\theta_i^2<0$, 这意味着存在非实的根. 在 $\theta_1\notin\mathbb{R}$ 的情形将有 $\overline{\theta_1}\neq\theta_1$, 从而我们至少有两个非实的根, 而根据构造, 这些根恰好有两个. 现在我们看到

$$f(X)=X^k+a_1X^{k-1}+\cdots+a_k,\quad a_i\in2\mathbb{Z}.$$

因为 $g(X)$ 的常数项被 4 整除, 所以 $f(X)$ 的常数项被 2 整除但不被 4 整除. 由艾森斯坦判别法, 将素数 2 用于 f 时推出 f 在 $\mathbb{Q}$ 上不可约. 因此, 定理 2 的条件对每一个素数 $p=k\geqslant5$ 都被满足. 当 $p=2$ 和 $p=3$ 时, 见例子. □

3. 以模 p 简化的方法 计算 $\mathrm{Gal}(f)(f \in \mathbb{Z}[X])$ 的重要辅助方法是以模 p 简化，其中 p 将走遍不相同的素数. 多项式 f 的系数的简化导致自然同态 $\mathbb{Z}[X] \to \mathbb{Z}_p[X]$. 我们将多项式 $f(X)$ 在这个同态下的像写成 $f_p(X)$. 因为判别式 $D(f)$ 是系数在 $\mathbb{Z}$ 中的多项式函数 (来自 f 的系数), 所以 $D(f) \in \mathbb{Z}$ 且 $D(f_p) = D(f)_p$. 若 $D(f_p) \neq 0$, 则 $D(f) \neq 0$,从而两个多项式 f, f_p (次数相同) 各自的根都不相同. 在这种情形有

定理 5 (戴德金) 设 $f \in \mathbb{Z}[X]$ 是 n 次标准多项式, p 是素数, $D(f_p) \neq 0$. 设 $f_p(X)$ 分解成 Z_p 上 $n_1, n_2, \cdots, n_r(\sum\limits_i n_i = n)$ 次不可约因式的乘积.

则伽罗瓦群 $\mathrm{Gal}(f)$ 含有作用在多项式 f 的根的集合上的置换, 这个置换在将根作适当的排序后有下列循环结构

$$(1, 2, \cdots, n_1)(n_1 + 1, \cdots, n_1 + n_2)(n_1 + n_2 + 1, \cdots, n_1 + n_2 + n_3) \cdots$$

为了证明这个重要的定理将先作出一些辅助性的断言. 我们从关于特征标的线性无关性的经典结果开始. 设 H 是幺半群, K 是域. H 到 K 的特征标 χ (或幺半群 H 的 K–特征标) 是指同态 $H \to K^*$ $(\chi(1) = 1,\ \chi(ab) = \chi(a)\chi(b))$.

引理 1 (关于无关性的戴德金–阿廷引理) 幺半群 H 到域 K 的不相同的特征标 $\chi_1, \chi_2, \cdots, \chi_n$ 在 K 上线性无关, 即

$$\sum_i a_i \chi_i(h) = 0, \quad a_i \in K, \quad \forall h \in H \Longrightarrow a_i = 0, \quad 1 \leqslant i \leqslant n.$$

证明 对 n 用归纳法. 若 $n = 1$, 则结果是明显的, 这是因为 $a\chi(h) = 0, a \neq 0$ 意味着对任意 $h \in H, \chi(h) = 0$, 然而这时根据条件, $\chi(1) = 1$.

现在设 $n > 1$, 并设已对 $n - 1$ 确立了无关性. 我们认为所有的 $a_i \neq 0$, 否则用归纳假定就行了. 因为 $\chi_1 \neq \chi_2$, 所以对某个 $h' \in H$ 有 $\chi_1(h') \neq \chi_2(h')$. 我们在假定的线性相关性式中用 $h'h$ 代替 h. 这就导致关系式

$$a_1\chi_1(h')\chi_1(h) + a_2\chi_2(h')\chi_2(h) + \cdots + a_n\chi_n(h')\chi_n(h) = 0.$$

另一方面, 用 $\chi_1(h')$ 乘原来的式子, 我们将有

$$a_1\chi_1(h')\chi_1(h) + a_2\chi_1(h')\chi_2(h) + \cdots + a_n\chi_1(h')\chi_n(h) = 0.$$

从第一个式子中减去后一个式子, 我们得到

$$a'_2\chi_2(h) + \cdots + a'_n\chi_n(h) = 0,$$

其中

$$a'_i = a_i(\chi_i(h') - \chi_1(h')), \quad 2 \leqslant i \leqslant n.$$

因为 $a'_2 = a_2(\chi_2(h') - \chi_1(h')) \neq 0$, 所以与归纳假定矛盾. □

推论 1 设 K_1, K_2 是两个域, 且 $\eta_1, \cdots, \eta_n$ 是不相同的单同态 $K_1 \to K_2$. 则它们在 K_2 上线性无关.

证明 将 η_i 限制在 K_1^* 上并命 $H = K_1^*$. □

推论 2 (阿廷定理) 设 G 是域 F 的有限自同构群. 则 F 是在 G 的作用下不动的元素组成的子域 P 的伽罗瓦扩张且 $\operatorname{Gal} F/P = G$. □

下面的引理 2 是定理 5 的证明的基础.

引理 2 设 $f \in \mathbb{Z}[X]$ 是 n 次标准多项式, F 是它在 $\mathbb{Q}$ 上的分裂域, p 是使 $D(f_p) \neq 0$ 的素数, 即 f_p 在它自己在 Z_p 上的分裂域 $F_{(p)}$ 中的根不相同. 设 L 是 F 的子环, 它由多项式 f 的根生成. 则

a) 存在同态 $\psi : L \to F_{(p)}$;

b) 任意一个这样的同态确立了多项式 f 在 F 中的根的集合 R 到 f_p 在 $F_{(p)}$ 中的根的集合 R_p 的一个双射;

c) 若 ψ, ψ' 是两个这样的同态, 则 $\psi' = \psi \cdot \sigma$, 其中 $\sigma \in \operatorname{Gal} F/\mathbb{Q}$.

证明 根据条件,

$F = \mathbb{Q}(\theta_1, \cdots, \theta_n)$, $\quad f(X) = \prod_{i=1}^{n} (X - \theta_i)$ 在 $F[X]$ 中. 根据定义, $L = \mathbb{Z}[\theta_1, \cdots, \theta_n]$. 命

$$L' = \sum_{0 \leqslant k_i \leqslant n-1} \mathbb{Z}\theta_1^{k_1} \cdots \theta_n^{k_n}$$

是元素

$$\theta_1^{k_1} \cdots \theta_n^{k_n}, \quad 0 \leqslant k_i \leqslant n-1$$

的 $\mathbb{Z}$ 线性组合的集合. 因为 $f(\theta_i) = 0$, 所以 θ_i^n 是 $1, \theta_i, \theta_i^2, \cdots, \theta_i^{n-1}$ 的 $\mathbb{Z}$ 线性组合. 因此, $\theta_i L' \subset L'$, 并且对于任何正指数 $k_1, \cdots, k_n$, 根据迭代, 有 $\theta_1^{k_1} \cdots \theta_n^{k_n} L' \subset L'$. 这就是说, L' 是 L 的子域, 根据定义, 它含有 $\theta_1, \cdots, \theta_n$, 因此它和 L 相等.

这表明 L 是有限生成 $\mathbb{Z}$–模. 因为 $\operatorname{char} F = 0$, 所以挠 $\operatorname{Tor} L$ 等于零, 从而 L 是有基 $(u_1, \cdots, u_m)$ 的有限秩自由 $\mathbb{Z}$–模: $L = \mathbb{Z}u_1 \oplus \cdots \oplus \mathbb{Z}u_m$.

我们断言, (u_i) 是扩张 $F/\mathbb{Q}$ 的基, 因此 $[F : \mathbb{Q}] = m$. 元素 u_i 在 $\mathbb{Q}$ 上的线性无关性是显然的, 这是因为 u_i 之间的非平凡 $\mathbb{Q}$-线性相关性导致 (当用某个整数来乘时) 非平凡的 $\mathbb{Z}$–线性相关性, 而事实上这是不存在的. 现在我们考察 F 中包含 $\mathbb{Q}$ 的子环 $\mathbb{Q}L = \sum_i \mathbb{Q}u_i$. 由 F 的代数性推出 $\mathbb{Q}L$ 是 F 的子域 (见 §1 中定理 2 的推论). 因为它包含所有 $\theta_i, 1 \leqslant i \leqslant n$, 所以 $\mathbb{Q}L = F$. 于是 (u_i) 是 $F/\mathbb{Q}$ 的基.

我们来考察环 L 的理想 $pL = \sum_{i=1}^{m} \mathbb{Z}(pu_i)$. 显然, $|L/pL| = p^m$. 因为商环 L/pL 是有限环, 所以显然它有 M/pL 这种形状的极大真理想, 其中 M 是 L 中包含 pL 的极大理想. 在这种情形, L/M 是域, 它是环 L/pL 的同态像, 这是因为根据同构

定理 (见第 4 章) 当中的一个, 我们有 $(L/pL)/(M/pL) \cong L/M$. 由构造明显看出, $\operatorname{char} L/M = p$, 且 Z_p 是 L/M 的素子域, 而 $|L/M| = p^{m'}$, 其中 $m' \leqslant m$.

a) 自然同态 $\nu : L \to L/M$ 将 $\mathbb{Z}$ 映到素域 Z_p (或者如果乐意的话, 到 $\mathbb{F}_p$) 上, 而因为 $L = \mathbb{Z}[\theta_1, \cdots, \theta_n]$ 并且在 $L[X]$ 中有 $f(X) = \prod_{i=1}^{n}(X - \theta_i)$, 所以 $L/M = Z_p[\overline{\theta}_1, \cdots, \overline{\theta}_n]$, 其中 $\overline{\theta}_i = \nu(\theta_i) = \theta_i + M$. 又, 由 $f \in \mathbb{Z}[X]$ 推出多项式 $\overline{f}(X) = \prod_{i=1}^{n}(X - \overline{\theta}_i)$ 的系数属于 Z_p 且 $\overline{f}(X) = f_p(X)$. 因此, L/M 是 $f_p(X)$ 在 Z_p 上的分裂域, 从而我们有同构 $\mu : L/M \to F_{(p)}$. 于是, 我们得到所需要的满同态 $\psi = \mu \circ \nu : L \to F_{(p)}$.

b) 设 ψ 是在 a) 中所确立的那种同态. 则限制 $\psi|_{\mathbb{Z}}$ 将是 $\mathbb{Z}$ 到 $F_{(p)}$ 的素子域上的同态, $\psi(1) = 1_{F_{(p)}}$, 于是 $\psi|_{\mathbb{Z}}$ 是 $\mathbb{Z}$ 到 Z_p 上的自然同态. 在这种情形, $f_p(X) = \psi(f(X)) := \prod_i (X - \psi(\theta_i))$. 因此, $\psi(\theta_i)$ 是多项式 $f_p(X)$ 在 $F_{(p)}$ 中的根且 $\psi|_R$ 是 R 到 R_p 上的双射.

c) 我们固定一个同态 $\psi : L \to F_{(p)}$. 设 $\sigma \in G = \operatorname{Gal} F/\mathbb{Q}$. 则 σ 对 θ_i 作了一个置换, 因此 σ 将 L 映入自身. 又, $\sigma|_L$ 是 L 到 L 的同态 (实际上是自同构), 而 $\psi \circ \sigma$ 是 L 到 $F_{(p)}$ 的同态. 不相同的 $\sigma, \sigma' \in G$ 给出根 θ_i 的不相同的置换, 而由于 $\psi|_R$ 是到 R_p 上的双射, $\psi \circ \sigma$ 和 $\psi \circ \sigma'$ 不相同. 若 $G = \{\sigma_1, \cdots, \sigma_m\}$, 则我们用这种方法得到 $m = [F : \mathbb{Q}]$ 个不相同的同态 $\psi_j = \psi \circ \sigma_j$.

我们断言, 再也没有其它的同态. 事实上, 设 ψ_{m+1} 和 ψ_j 不相同, $1 \leqslant j \leqslant m$. 将引理 1 应用于 L 的乘法幺半群 H 及域 $K = F_{(p)}$, 可知, 包括 ψ_{m+1} 在内的所有的 ψ_j 在 $F_{(p)}$ 上线性无关. 另一方面, 我们来考察方程组

$$\sum_{i=1}^{m+1} x_i \psi_i(u_j) = 0, \quad 1 \leqslant j \leqslant m.$$

因为未知量 x_i 比方程多, 所以系数 $\psi_i(u_j) \in F_{(p)}$ 的这个齐次线性方程组有非平凡解 $(a_1, \cdots, a_{m+1}), a_i \in F_{(p)}$. 现在设 $y \in L$. 则 $y = \sum_j n_j u_j, n_j \in \mathbb{Z}$, 且

$$\psi_i(y) = \sum_j \overline{n_j} \psi_i(u_j), \quad \overline{n}_j = n_j + p\mathbb{Z};$$

$$\sum a_i \psi_i(y) = \sum_j \overline{n_j} \left(\sum_i a_i \psi_i(u_j) \right) = \sum_j \overline{n}_j(0) = 0.$$

这和 ψ_i 的无关性矛盾, 从而完成了 c) 的证明. □

最后, 我们已准备好了来给出

定理 5 的证明 因为 $F_{(p)}$ 是有 p^m 个元素的域, 所以映射 $\pi : a \mapsto a^p, a \in F_{(p)}$ 是自同构. 若 $\psi : L \to F_{(p)}$ 是任意同态, 则 $\pi \circ \psi$ 也是同态. 相应地我们有唯一的元素 $\sigma = \sigma(\psi) \in \operatorname{Gal}(f)$, 使得

$$\pi \circ \psi = \psi \circ \sigma(\psi).$$

自同构 $\sigma = \sigma(\psi)$ 叫做对应于 ψ 的 $F/\mathbb{Q}$ 上**弗罗贝尼乌斯 p–自同构**.

如果我们将 ψ 及 σ 限制在 R 上并且利用 ψ 是 R 到 R_p上的双射这一事实, 则得到关系式 $\sigma = \psi^{-1} \circ \pi \circ \psi$. 这意味着 R_p 上关于 $\langle\pi\rangle$ 的轨道利用 ψ^{-1} 被映射到 R 上关于 $\langle\sigma\rangle$ 的轨道.

但是 R_p 上关于 $\langle\pi\rangle$ 的轨道是多项式 $f_p \in Z_p[X]$ 的不可约因式的根的集合. 若 $n_1, \cdots, n_r$ 是这些多项式的次数, 则 R 上关于 $\langle\sigma\rangle$ 的轨道的势将是 $n_1 \cdots n_r$, 因此, σ 作为 R 上的置换在对根作适当排序后有循环分解

$$(1\ 2 \cdots n_1)(n_1 + 1, \cdots n_1 + n_2) \cdots . \qquad \square$$

例 3 设 $f(X) = X^6 + 22X^5 + 21X^4 + 12X^3 - 37X^2 - 29X - 15$. 首先我们模 2 进行化简以得到

$$f_2(X) = X^6 + X^4 + X^2 + X + 1.$$

被次数 $\leqslant 3$ 的不可约多项式 $X^2 + X + 1, X^3 + X^2 + 1, X^3 + X + 1$ 整除是不可能的, 因此 $f_2(X)$ 是不可约的. 从而 $\mathrm{Gal}(f)$ 含有 6-循环. 于是 $\mathrm{Gal}(f)$ 是可迁的. 又

$$f_3(X) = X\left(X^5 + X^4 - X + 1\right),$$

并且 $X^5 + X^4 - X + 1$ 模 3 是不可约的. 于是 $\mathrm{Gal}(f)$ 含有 5-循环. 最后

$$f_5(X) = X(X-1)(X+1)(X+2)\left(X^2 + 2\right)$$

及 $X^2 + 2$ 模 5 是不可约的. 因此 $\mathrm{Gal}(f)$ 含有 2-循环. 根据命题 1, 我们得到结论: $\mathrm{Gal}(f) \cong S_b$.

为了在定理 5 的基础上构造次数 $n > 3$ 的多项式 $f \in \mathbb{Z}[X]$ 使 $\mathrm{Gal}(f) \cong S_n$, 我们首先取模 2 不可约的 n 次多项式 $u \in \mathbb{Z}[X]$; 然后取模 3 分解成一个 $n-1$ 次不可约多项式和一个线性因式之积的多项式 $v \in \mathbb{Z}[X]$; 最后, 我们取模 5 分解成一个 2 次不可约因式和一个或若干个奇数次不可约因式之积的多项式 $w \in \mathbb{Z}[X]$. 所有这些都是可能的, 这是因为模任何素数, 总存在有事先任意给定次数的不可约多项式.

最后, 我们取多项式 f 使满足条件

$$f \equiv u (\operatorname{mod} 2), \quad f \equiv v (\operatorname{mod} 3), \quad f \equiv w (\operatorname{mod} 5).$$

只要命

$$f = -15u + 10v + 6w$$

就可以了 (所有多项式都是标准的).

这时群 $\mathrm{Gal}(f)$ 将是可迁的 (f 模 2 不可约), 含有 $(1\ 2 \cdots n-1)$ 这种类型的一个循环置换并含有一个对换和长度为奇数的不相交轮换的积. 若后面这一个乘积取适当的奇次幂, 则得到纯对换. 由命题 1, 我们得到 $\mathrm{Gal}(f) \cong S_n$.

在本节第 2 目中一开始就提到过的 I. 舒尔关于同构于 S_n 的伽罗瓦群的具体多项式的结果并不会使定理 5 逊色. 以它为基础的计算用于别的情况.

4. 正规基 设 F 是 P 上任意伽罗瓦扩张, 且 $\mathrm{Gal}\,F/P = G = \{\eta_i | 1 \leqslant i \leqslant n\}, n = [F:P]$. 如果 $z \in F$ 且 $\{z_1, z_2, \cdots, z_m\} = Gz$ 是在 G 作用下的轨道, 则 z 在 P 上的极小多项式将是 $\prod_1^m (X - z_i)$. 因此, z 是本原元素当且仅当 $m = |Gz| = n$. 更强的性质: 元素 $\eta_1(z), \eta_2(z), \cdots, \eta_n(z)$ 不仅不相同, 而且在 P 上线性无关. 如果是这样, 则 $(\eta_1(z), \cdots, \eta_n(z))$ 是 F/P 的基, 它叫做给定扩张的**正规基**. 正规基的存在性的证明基于下面的判别法.

命题 3 设 K/P 是有限维可分扩张, L/P 是它的正规闭包, 则

1) 单同态 $K/P \to L/P$ 的个数等于 $n = [K:P]$;

2) 若 $1 = \eta_1, \eta_2, \cdots, \eta_n$ 是这些单同态, 则 $\{u_1, u_2, \cdots, u_n\}\,(u_i \in K)$ 是 K/P 的基当且仅当

$$\begin{vmatrix} u_1 & u_2 & & u_n \\ \eta_2(u_1) & \eta_2(u_2) & \cdots & \eta_2(u_n) \\ \cdots & \cdots & \cdots & \cdots \\ \eta_n(u_1) & \eta_n(u_2) & \cdots & \eta_n(u_n) \end{vmatrix} \neq 0$$

证明 1) 设 $G = \mathrm{Gal}\,L/P$, 并设 $H \subset G$ 是将 K 固定的子群. 则 $n = [K:P] = (G:H)$, 并且我们可以写出分解成左陪集的分解式 $G = \theta_1 H \cup \cdots \cup \theta_n H\,(\theta_1 = 1)$. 命 $\eta_i = \theta_i|_K$, 则 η_i 是单同态嵌入 $K/P \hookrightarrow L/P$ 且当 $i \neq j$ 时, $\eta_i \neq \eta_j$. 事实上, 若 $\eta_i = \eta_j$, 则 $\theta_i^{-1}(\theta_j(u)) = u, \forall u \in K$. 在这种情形, $\theta_i^{-1}\theta_j \in H$, 与假定相违.

现在设 η 是任意单同态 $K/P \hookrightarrow L/P$. 因为 L 是某一个多项式 $f \in P[X]$ 在 P 上的分裂域, 所以 L 将是这个多项式在 K 上的分裂域, 也是在 $\eta(K)$ 上的分裂域. 因此 (根据分裂域同构定理), 同构 $\eta: K \to \eta(K)$ 可以延拓成扩张 L/P 的自同构 θ. 换句话说, $\theta \in \mathrm{Gal}\,L/P$, 从而 $\theta = \theta_i\mu$ 对某个 $\mu \in H$. 但这时 $\eta = \theta|_K = \theta_i|_K = \eta_i$, 即 $\eta_1 = 1, \cdots, \eta_n$ 是单同态 $K/P \hookrightarrow L/P$ 的全部.

2) 假定有元素 $u_1, \cdots, u_n \in K$ 的一个非平凡线性相关式 $\sum_i a_i u_i = 0, a_i \in P$. 则当应用 η_j 后, 我们得到: 齐次线性方程组

$$\sum_{i=1}^n \eta_j(u_i)x_i = 0, \quad 1 \leqslant j \leqslant n,$$

有非零解 $(a_1, \cdots, a_n)$, 这意味着 $\det(\eta_j(u_i)) = 0$.

反之, 假定 $\det(\eta_j(u_i)) = 0$. 在这种情形, 齐次线性方程组 $\sum_j \eta_j(u_i)x_j = 0, 1 \leqslant i \leqslant n$ 有非零解 $(a_1, \cdots, a_n), a_i \in L$. 而这意味着 $(u_1, \cdots, u_n)$ 不是 K 的基: 若任意元素 $u \in K$ 写成 $\sum_i c_i u_i$ 的形状, $c_i \in P$, 且

$$\sum_j a_j \eta_j(u) = \sum_{i,j} a_j c_i \eta_j(u_i) = \sum_i \left(\sum_j a_j \eta_j(u_i) \right) = 0,$$

则这和单同态 $\eta_1, \cdots, \eta_n$ 的线性无关性 (戴德金–阿廷引理推论 1) 矛盾. □

命题 4 P 为有限域时, 伽罗瓦扩张 L/P 有正规基.

证明 在有限域 P 的情形, 扩张 L/P 将是循环的, 且

$$G = \operatorname{Gal} L/P = \langle\sigma\rangle = \left\{1, \sigma, \sigma^2, \cdots, \sigma^{m-1}\right\},$$

其中 $m = [L:P]$. 我们将 σ 解释成 P 上 L 的线性变换, 这是因为

$$\sigma(u+v) = \sigma(u) + \sigma(v), \sigma(au) = a\sigma(u), \quad a \in P.$$

大家知道, 由线性变换确定的 $P[X]$–模是具有零化子的循环子空间的直和, 这些零化子是不变因子 $d_1(X), \cdots, d_n(X)$, 其中 $d_s(X)$ 是线性变换的极小多项式 (所有不变因子的乘积是特征多项式). 整个 $P[X]$-模是循环的当且仅当特征多项式和极小多项式一致, 即极小多项式的次数和整个空间的维数一致.

对于 σ 的情形, 事情正是这样. 因为 $\sigma^m = 1$, 所 $X^m - 1$ 是特征多项式. 另一方面, 若

$$f(X) = X^k + a_1 X^{k-1} + \cdots + a_k, \quad a_i \in P, \quad k < m,$$

则 $f(\sigma) \neq 0$, 这是因为自同构 $1, \sigma, \cdots, \sigma^k$ 不相同, 从而在 L 上线性无关, 尤其是在 P 上线性无关.

L 是循环的 (作为 $P[X]$–模) 这一事实意味着 L/P 有 $(u, \sigma(u), \cdots, \sigma^{m-1}(u))$ 这种形状的基. 而这就是 L/P 的正规基. □

定义 设 K, L 是两个域. 一组单同态 $\eta_1, \eta_2, \cdots, \eta_n : K \hookrightarrow L$ 叫做**在 L 上代数无关的**, 如果

$$f \in L[X_1, \cdots, X_n], \quad f(\eta_1(u), \cdots, \eta_n(u)) = 0 \quad \forall u \in K \Longrightarrow f = 0.$$

命题 5 设 P 是无限域, K 是 P 上有限维可分扩张, L 是扩张 K/P 的正规闭包. 设 $\eta_1, \cdots, \eta_n$ 是 $n = [K:P]$ 个不相同的单同态 $K/P \hookrightarrow L/P$. 则 η_i 在 L 上代数无关.

证明 假定对某个 $f \in L[X_1, \cdots, X_n]$ 有 $f(\eta_1(u), \cdots, \eta_n(u)) = 0, \forall u \in K$. 设 (u_i) 是 K/P 的基, 则对任意选取的 $a_i \in P$, 我们有

$$0 = f\left(\eta_1\left(\sum_i a_i u_i\right), \cdots, \eta_n\left(\sum_i a_i u_i\right)\right) = f\left(\sum_i a_i \eta_1(u_i), \cdots, \sum_i a_i \eta_n(u_i)\right).$$

如果命

$$g(X_1, \cdots, X_n) = f\left(\sum \eta_1(u_i) X_i, \cdots, \sum \eta_n(u_i) X_i\right),$$

则 $g(a_1,\cdots,a_n)=0$ 对任意 $a_i\in P$. 设 $(v_1,v_2,\cdots,v_n)$ 是 L/P 的基, 则可以写成

$$g(X_1,\cdots,X_n)=\sum_{j=1}^{m}g_j(X_1,\cdots,X_n)v_j,$$

其中 $g_j(X_1,\cdots,X_n)\in P[X_1,\cdots,X_n]$. 条件 $g(a_1,\cdots,a_n)=0$ 可表示成 $g_j(a_1,\cdots,a_n)=0,\forall_j$. 因为这对所有 $a_i\in P$ 成立, 所以由多项式函数和无限域上多项式之间的对应推出 $g_j(X_1,\cdots,X_n)=0$, 于是 $g(X_1,\cdots,X_n)=0$.

基于命题 3, $\det(\eta_j(u_i))\neq 0$, 因此矩阵 $(\eta_j(u_i))$ 有逆 $(v_{ij})\in M_n(L)$. 这就是说

$$g\left(\sum_{j,k}v_{1j}\eta_j(u_k)X_k,\cdots,\sum_{j,k}v_{nj}\eta_j(u_k)X_k\right)=f(X_1,\cdots,X_n).$$

所以 $g(X_1,\cdots,X_n)=0\Longrightarrow f(X_1,\cdots,X_n)=0$. 这就证明了 η_i 在 L 上的代数无关性.

□

我们已经走近核心结果了.

定理 6 任意有限维伽罗瓦扩张 L/P 有正规基.

证明 基于命题 4, 域 P 可以认为是限的. 正如命题 5 指出的, 扩张 L/P 的自同构 $\eta_1,\cdots,\eta_n$ 在 L 上代数无关.

我们也看到过, 若 $u\in L$, 则

$$(\eta_1(u),\cdots,\eta_n(u))\text{ 是基}\Longleftrightarrow\det(\eta_i\eta_j(u))\neq 0.$$

命 $\eta_i\eta_j=\eta_{i(j)}$. 则 $j\mapsto i(j)$ 是作用在集合 $\{1,2,\cdots,n\}$ 上的一个置换. 现在我们来考察多项式代数 $L[X_1,\cdots,X_n]$ 及矩阵 $X=\left(x_{i(j)}\right)$. 我们断言 $\det X\neq 0$. 为此, 我们选取特殊的 $x_1=1,x_i=0,i>1$. 因为置换 $j\mapsto i(j)$ 对于不相同的 i 是不相同的, 所以 x_1 在矩阵 X 的每一行及每一列中出现一次而且只出现一次. 于是 $\det X(x_1=1,x_i=0,i>1)=\pm 1$. 尤其是 $\det X\neq 0$ 对任何 X.

基于 η_i 在 L 上的代数无关性, 存在 $u\in L$ 使 $\det((\eta_i\eta_j)(u))\neq 0$. 在这种情形, $(\eta_1(u),\cdots,\eta_n(u))$ 是正规基. □

用表示论的语言来说, 关于正规基的定理断言是伽罗瓦群在域 L 的加法群上 (在向量空间上) 的表示是正则的. 也可以说, L 是群环 $P[G]$ 上维数为 1 的自由模. 这样的结果可以看作是数的代数理论的非常精细的研究的第一步. 就是说, 设 L 是数域 (域 $\mathbb{Q}$ 的有限扩张), O_L 是 L 中代数整数的环. 要弄清 O_L 作为 $\mathbb{Z}[G]$-模的结构是一个困难的任务.

看来, 关于正规基的定理使伽罗瓦理论的群论部分失色: 正则表示并不是非常有意思的. 但是也应该注意到域的乘法结构以及这样一种情形, 即伽罗瓦群当作原来多项式的根的置换群, 而这个作用可以有本原性、多重传递性等性质.

习　题

1. 求扩张 $\mathbb{F}_8/\mathbb{F}_2$ 的正规基. 为确定起见, 我们认为 $\mathbb{F}_8=\mathbb{F}_2(\theta),\theta^3+\theta+1=0$.

2. 求扩张 $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ 的正规基.

§5 伽罗瓦扩张及相近的问题

1. 算术级数中的素数　由 §2 中分圆多项式的定义, 现在我们得到以引理的形式表述的两个简单的断言.

引理 1　*设 $a\neq 0$ 是整数, n 是不被素数 p 整除的自然数. 则*

$$p|\Phi_n(a)\Longleftrightarrow\{a \text{ 在 } Z_p^* \text{ 中有周期 } n\}$$

(等价地: $a^n\equiv 1(\bmod p), a^m\not\equiv 1(\bmod p), \forall m<n$).

证明　我们考察分解式

$$X^n-1=\Phi_n(X)\prod_{d|n,d<n}\Phi_d(X)\in Z_p^*[X]. \tag{$*$}$$

1) 若在 Z_p 中 $\Phi_n(a)=0$, 则根据 $(*)$, 在 Z_p 中有 $a^n-1=0$. 若此外对某个 $m|n,m<n$ 还有 $\Phi_m(a)=0$, 则 $X^n-1=(X-a)^2f(X)$. 但是微商 $(X^n-1)'=nX^{n-1}$ 和 X^n-1 互素, 这是因为在 Z_p 中 $n\neq 0$. 因此 X^n-1 没有重根. 这意味着 a 不可能是多项式 X^m-1 的根, 其中 $m<n,m|n$, 这是因为 $X^m-1=\prod\limits_{d|m,d<n}\Phi_d(X)$. 这就是说, a 有周期 n.

2) 反之, 现在设 a 在 Z_p^* 中有周期 n. 若对某个 $d|n,d<n$ 有 $\Phi_d(a)=0$, 则正如我们在 1) 中已经看到过, 在 Z_p^* 中有 $a^d=1$. 矛盾. 只剩下 $\Phi_n(a)=0$ (即 $p|\Phi_n(a)$) 这一种可能性. □

引理 2　*设 $n\in\mathbb{Z}$, p 是不整除 n 的素数. 则*

$$\text{对某个 } a\in\mathbb{Z},\quad \Phi_n(a)\equiv 0(\bmod p)\Longleftrightarrow p\equiv 1(\bmod n).$$

证明　根据引理 1, $\Phi_n(a)\equiv 0(\bmod p)\Longrightarrow a^n\equiv 1(\bmod p)$, 并且 n 是元素 a 的周期. 但这时 $n\leqslant p-1$, 这是因为恒有 $a^{p-1}\equiv 1(\bmod p)$, 且 $n|(p-1)$, 即 $p\equiv 1(\bmod n)$.

反之, 若 $p\equiv 1(\bmod n)$, 则基于 Z_p^* 的循环性, 存在 $a\in\mathbb{Z}$, 它在 Z_p^* 中的周期是 n. 重新又根据引理 1, 我们有 $\Phi_n(a)\equiv 0(\bmod p)$. □

定理 1 (狄利克雷定理的特殊情形)　*在算术级数 $kn+1,k=1,2,\cdots$, 中存在无限多个素数.*

证明 事实上, 对于任何一个固定的 $n > 1$, 我们有

$$\Phi_n(a) = a^m + \alpha_1 a^{m-1} + \cdots + \alpha_{m-1}a + 1, \quad m = \varphi(n).$$

假定只存在素数的有限集 $M = \{p_1, \cdots, p_s\}$ 使得对所有充分大的自然数 a 有 $\Phi_n(a) \equiv 0 (\mathrm{mod}\, p_i), i = i(a)$. 然而对 $a = (p_1 p_2 \cdots p_s)^N, N \gg 0$, 将有 $\Phi_n(a) \equiv 1 (\mathrm{mod}\, p_i), 1 \leqslant i \leqslant s$. 矛盾.

于是, 存在无限多个素数 p 使得当适当地选取自然数 $a = a_p$ 时, 有 $\Phi_n(a) \equiv 0 (\mathrm{mod}\, p)$. 根据引理 2, 我们得到 $p \equiv 1 (\mathrm{mod}\, n)$ 对每一个这样的素数 p.

2. 伽罗瓦群为交换群的扩张 一个扩张叫做是**循环的, 交换的, 可解的**, 是指当相应的伽罗瓦群是循环的, 交换的或可解的. 具有给定阶的有限交换群一般说是相当多的, 因此, 从伽罗瓦理论的角度来看一看它们是有意思的.

定理 2 *设 A 是任意有限交换群. 则存在正规扩张 $F/\mathbb{Q}$, 其伽罗瓦群*

$$\mathrm{Gal}\, F/\mathbb{Q} \cong A.$$

证明 根据有限交换群的结构的基本定理 (第 2 章 §3 定理 10),

$$A = A_1 \times A_2 \times \cdots \times A_k,$$

其中 $A_j = \langle u_j \rangle$ 是 m_j 阶循环群, $1 \leqslant j \leqslant k$, 并且 $m_1 | m_2, \cdots, m_{k-1} | m_k$. 整数 m_j 叫做群 A 的**不变因子**. 显然,

$$|A| = m_1 m_2 \cdots m_k.$$

根据定理 1, 存在两两不相同的素数

$$p_1, p_2, \cdots, p_k \ (p_i \neq p_j \text{ 即使 } m_i = m_j)$$

使

$$p_j - 1 = n_j m_j.$$

现在我们考察相应于整数 $n = p_1 p_2 \cdots p_k$ 的分圆域 $\Gamma_n = \mathbb{Q}(\zeta), \zeta^n = 1$, 于是

$$\begin{aligned}[\Gamma_n : \mathbb{Q}] = \varphi(n) &= \varphi(p_1)\varphi(p_2)\cdots\varphi(p_k) \\ &= (p_1 - 1)(p_2 - 1)\cdots(p_k - 1) = n_1 m_1 n_2 m_2 \cdots n_k m_k.\end{aligned}$$

我们看到, 若 F_1, F_2 是域 F 的两个子域, 则含有 F_1 和 F_2 的最小子域记作 $F_1 \cdot F_2$ 并叫做域 F_1, F_2 的**合成**. 又

$$\Gamma_s \cap \Gamma_t = \mathbb{Q} \text{ 当 } \mathrm{g.c.d}\,(s, t) = 1, \text{ 且 } \Gamma_s \Gamma_t = \Gamma_{st}.$$

在我们的情形,

$$\Gamma_n = \Gamma_{p_1} \cdot \Gamma_{p_2} \cdots \Gamma_{p_k},$$

其中

$$\Gamma_{p_j} = \mathbb{Q}(\zeta_j), \quad \zeta_j = \zeta^{p_1 \cdots \hat{p}_j \cdots p_k}, \zeta_j^{p_j} = 1.$$

现在显然有

$$\left\{\mathrm{Gal}\Gamma_{p_j}/\mathbb{Q}\right\} \cap \left\{\prod_{i \neq j} \mathrm{Gal}\,\Gamma_{p_i}/\mathbb{Q}\right\} = \langle 1 \rangle.$$

因此,

$$\begin{aligned}
&\mathrm{Gal}\,\Gamma_n/\mathbb{Q} = \mathrm{Gal}\,\Gamma_{p_1}/\mathbb{Q} \times \cdots \times \mathrm{Gal}\,\Gamma_{p_k}/\mathbb{Q} = \langle \sigma_1 \rangle \times \cdots \times \langle \sigma_k \rangle := G, \\
&\qquad \sigma_j \ : \ \zeta_j \mapsto \zeta_j^{a_j}, \quad \langle a_j \rangle = Z_{p_j}^*, \quad |\langle \sigma_j \rangle| = n_j m_j; \\
&\qquad \sigma_j \ : \ \zeta_i \mapsto \zeta_j, \quad i \neq j.
\end{aligned}$$

群 G 含有子群

$$H = \langle \sigma_1^{m_1} \rangle \times \cdots \times \langle \sigma_k^{m_k} \rangle,$$

其阶为 $n_1 \cdots n_k$. 显然, $H \lhd G$, 并且商群

$$G/H = \langle \overline{\sigma}_1 \rangle \times \cdots \times \langle \overline{\sigma}_k \rangle, \quad \overline{\sigma}_j = \sigma_j \left(\sigma_j^{m_j}\right)$$

(它是阶为 $m_1, \cdots, m_k$ 的循环群的直积) 和 A 同构. 若现在 $F = \Gamma_n^H$ 是 Γ_n 中 H–不变元 (在 H 作用下不动的元素) 作成的子域, 则基于伽罗瓦对应, 有

$$\mathrm{Gal}\,F/\mathbb{Q} \cong G/H \cong A. \qquad \square$$

3. 范数与迹 设 F/P 是伽罗瓦扩张,

$$G = \mathrm{Gal}\,F/P = \langle \eta_1 = 1, \eta_2, \cdots, \eta_n \rangle.$$

对于 $u \in F$, 我们命

$$T_P^F(u) = \sum_{i=1}^{n} \eta_i(u), \quad N_P^F(u) = \prod_{i=1}^{n} \eta_i(u)$$

并把它们相应地叫做**元素 u 在 F/P 中的迹和范数**. 显然, 它们关于 G 是不动的, 从而它们在 P 中. 因此, 我们有 F 到 P 的映射

$$T_P^F : u \mapsto T_P^F(u), \quad N_P^F : u \mapsto N_P^F(u).$$

对于 $u, v \in F, a \in P$, 我们有

$$
\begin{aligned}
T_P^F(u+v) &= \sum_i \eta_i(u+v) = \sum_i \eta_i(u) + \sum_i \eta_i(v) = T_P^F(u) + T_P^F(v), \\
T_P^F(au) &= \sum_i \eta_i(au) = a \sum_i \eta_i(u) = a \cdot T_P^F(u), \\
N_P^F(uv) &= \prod_i \eta_i(uv) = \prod_i \eta_i(u) \prod_i \eta_i(v) = N_P^F(u) \cdot N_P^F(v), \\
N_P^F(au) &= \prod_i \eta_i(au) = a^n \prod_i \eta_i(u) = a^n \cdot N_P^F(u).
\end{aligned}
$$

于是, $T = T_P^F$ 是 P 上向量空间 F 上的线性函数; $N = N_P^F$ 是 n 次乘性齐次映射; $N|_{F^*}$ 是 F^* 到 P^* 的同态.

例 1 设 m 是不含平方因子的整数, $F = \mathbb{Q}(\sqrt{m})$ 是二次域. 则 $u = a + b\sqrt{m}$ 是 F 中元素的一般形状, $a, b \in \mathbb{Q}$, 且

$$
G = \operatorname{Gal} F/\mathbb{Q} = \{1, \eta : a + b\sqrt{m} \mapsto a - b\sqrt{m}\},
$$

即 $T(a+b\sqrt{m}) = 2a, N(a+b\sqrt{m}) = a^2 - mb^2$. 当 $N(u) = a^2 + b^2$ 是复数的模的平方时, 与扩张 $\mathbb{C}/\mathbb{R}$ 完全类似, $m = -1$.

在我们的情形, 显然 $T(F) = \mathbb{Q}$. 想了解 $N(F^*)$ 的情况相当困难, 这是因为产生了不平凡的问题: 对于什么样的有理数 r, 方程 $x^2 - my^2 = r$ 在 $\mathbb{Q}$ 中有解?

有关于 $\operatorname{Ker} N$ 及 $\operatorname{Ker} T$ 的两个定理. 其中最著名的是下面的

定理 3 (希尔伯特定理 90, 1897 年) 设 F 是域 P 的循环伽罗瓦扩张, $G = \operatorname{Gal} F/P = \langle \eta \rangle, |G| = n$. 则

$$
N_P^F(u) = 1 \text{ 对 } u \in F \Longleftrightarrow u = v(\eta(v))^{-1} \text{ 对某个 } v \in F.
$$

结果的一面是平凡的: 若 $u = v(\eta(v))^{-1}$, 则 $N(u) = N(v) \cdot N(\eta(v)^{-1}) = N(v) \cdot N(v)^{-1} = 1$. 为了证明反过来的一面, 我们建立关于伽罗瓦扩张的更一般的 (更迟的) 结果.

定理 4 (施派泽 (Speiser)) 设 F 是域 P 的有限维伽罗瓦扩张, $G = \operatorname{Gal} F/P$. 设 $\zeta \mapsto u_\zeta$ 是 G 到 F^* 的映射, 它满足条件

$$
u_{\zeta\mu} = \zeta(u_\mu) u_\zeta \quad \forall \mu, \zeta \in G.
$$

则存在 $0 \neq v \in F$ 使

$$
u_\mu = v(\mu(v))^{-1} \quad \forall \mu \in G.
$$

证明　因为 $u_\mu \neq 0$, 而自同构 $\mu \in G$ 在 F 上线性无关, 所以存在元素 $w \in F$, 使

$$v = \sum_{\mu \in G} u_\mu \mu(w) \neq 0.$$

于是对任何 $\zeta \in G$, 有

$$\begin{aligned}\zeta(v) &= \sum_\mu \zeta(u_\mu)(\zeta\mu)(w) = \sum_\mu u_{\zeta\mu} u_\zeta^{-1} (\zeta\mu)(w) \\ &= \left(\sum_\mu u_{\zeta\mu}(\zeta\mu)(w)\right) u_\zeta^{-1} = \sum_\mu u_\mu \mu(w) u_\zeta^{-1} = v u_\zeta^{-1}.\end{aligned}$$

因此, $u_\zeta = v(\zeta(v))^{-1}$. □

希尔伯特定理的证明　设 $u \in F, N(u) = 1$. 我们命

$$u_\eta := u, \quad u_{\eta^i} := u\eta(u)\eta^2(u)\cdots\eta^{i-1}(u), \quad 1 \leqslant i \leqslant n.$$

则当 $i + j \leqslant n$ 时, 我们将有

$$u_{\eta^j} \cdot \eta^j(u_{\eta^j}) = u\eta(u)\cdots\eta^{j-1}\eta^j(u)\cdots\eta^{i+j-1}(u) = u_{\eta^{i+j}}.$$

当 $i + j > n$ 时, 同样的关系式也成立, 这是因为 $u_1 = u_{\eta^n} = N(u) = 1$. 因此, 对于 $G = \langle\eta\rangle$, 定理 4 的条件被满足, 由此推出存在元素 v, 它有所需要的性质 $u = u_\eta = v(\eta(v))^{-1}$. □

已被证明了的定理有加法型的类似结果.

定理 5 (施派泽)　*设 F, P, G 和乘法型定理 4 中的一样, 并设 $\mu \mapsto d_\mu$ 是 $G \to F$ 的映射, 它满足条件*

$$d_{\zeta\mu} = d_\zeta + \zeta(d_\mu) \quad \forall \zeta, \mu \in G.$$

则存在 $c \in F$, 使

$$d_\mu = c - \mu(c), \quad \mu \in G.$$

证明　我们看到过, 存在 $u \in F$ 使 $T(u) \neq 0$. 命

$$c = T(u)^{-1} \sum_\mu d_\mu \mu(u).$$

则

$$\begin{aligned}c - \zeta(c) &= T(u)^{-1} \sum_\mu [d_\mu \mu(u) - \zeta(d_\mu) \cdot \zeta\mu(u)] \\ &= T(u)^{-1} \sum_\mu [d_\mu \mu(u) + d_\zeta \cdot \zeta\mu(u) - d_{\zeta\mu} \cdot \zeta\mu(u)] \\ &= T(u)^{-1} d_\zeta \sum_\mu \zeta\mu(u) = d_\zeta T(u)^{-1} \sum_\sigma \sigma(u) = d_\zeta T(u)^{-1} T(u) = d_\zeta.\end{aligned}$$

元素 $\zeta \in G$ 是任意的. □

现在设 $G=\langle\eta\rangle, |G|=n$, 并假定元素 $d\in F$ 使 $T(d)=0$. 命

$$d_\eta := d, \quad d_{\eta^i} := d+\eta(d)+\cdots+\eta^{i-1}(d), \quad 1\leqslant i\leqslant n.$$

则正如希尔伯特定理在范数的情形一样, 有加法型施派泽定理的结论. 事实上,

$$d_1 = d_{\eta^n} = d+\eta(d)+\cdots+\eta^{n-1}(d)=T(d)=0.$$

因此, 对于任意 i,j, 有

$$d_{\eta^i\eta^j}=d_{\eta^{i+j}}=d+\eta(d)+\cdots+\eta^{i-1}+\eta^i\left[d+\eta(d)+\cdots+\eta^{j-1}(d)\right]=d_{\eta^i}+\eta^i\left(d_{\eta^j}\right),$$

即 $d_{\zeta\mu}=d_\zeta+\zeta(d_\mu), \forall\zeta,\mu\in G$, 并根据定理 5, 有 $d_\mu=c-\mu(c), \mu\in G$. 于是, 下面的定理 6 成立.

定理 6 (加法型希尔伯特定理 90) 设 F/P 是 n 次循环扩张, 其伽罗瓦群 $\operatorname{Gal} F/P=\langle\eta\rangle, d\in F$ 的迹为 0. 则存在 $c\in F$ 使 $d=c-\eta(c)$.

4. 循环扩张 现在我们将希尔伯特定理 90 及其加法型应用于最简型扩张.

定理 7 设 P 含有 1 的 n 个不相同的 n 次根. 下面的断言成立.

1) 设 F/P 是 n 维循环扩张. 则 $F=P(u)$, 其中 $u^n\in P$.

2) 设 $X^n-a\in P[X]$ 且 u 是多项式 X^n-a 的某个根, 则 $P(u)/P$ 是 m 次循环扩张, $m|n$ 且 $u^m\in P$.

证明 1) 由定理的条件推出, 域 P 的特征和 n 互素. 设 $\zeta\in P, \zeta^n=1, \zeta^i\neq 1, i<n$, η 是伽罗瓦群的生成元. 根据条件有 $\eta^i(\zeta)=\zeta, 0\leqslant i\leqslant n-1$, 于是 $N_P^F(\zeta)=\zeta^n=1$. 因此, 根据定理 3, 存在 $u\in F$ 使 $\zeta=u/\eta(u)$. 在这种情形, $\eta(u)=\zeta^{-1}u$ 且 $\eta(u^n)=\eta(u)^n=\left(\zeta^{-1}u\right)^n=u^n$, 由此推出 $u^n=a\in P$. 此外, $\eta(u)=\zeta^{-1}u\Longrightarrow\eta^i(u)=\zeta^{-i}u$, 于是元素 u 的 $\operatorname{Gal} F/P$–轨道含有 n 个不相同的元素. 因此, 元素 u 在 P 上的极小多项式有次数 n 且 $F=P(u)$.

2) 反之, 设 $a\in P, u^n=a, \zeta$ 是 1 的 n 次本原根. 因为 $\left(\zeta^i u\right)^n=a, i=0,1,\cdots,n-1$, 所以多项式 X^n-a 的全部根都在 $P(u)$ 中, 即 $P(u)$ 在 P 上是正规的.

命 $G=\operatorname{Gal} P(u)/P$. 若 $\eta\in G$, 则 $(\eta(u))^n=a$, 由此推出 $\eta(u)=\zeta^{i(\eta)}u$. 不难验证, 映射 $\eta\mapsto\zeta^{i(\eta)}$ 是 G 到群 $\langle\zeta\rangle$ 中的单同态. 但循环群的每一个子群都是循环群, 因此 G 是循环群, 并且若 $|G|=m$, 则 $m|n$. 命 $G=\langle\sigma\rangle$, 我们看出 $\zeta^{i(\sigma)}=\zeta^{n/m}$ 将是 1 的 m 次本原根. 最后,

$$\sigma\left(u^m\right)=(\sigma(u))^m=\left(\zeta^{n/m}u\right)^m=u^m,$$

于是 $u^m\in P$. □

推论 设 $a \neq b^m$ 对于不管怎样的 $m|n, m \neq 1, b \in P$, 并设和以前一样, $w^n = 1 \Longrightarrow w \in P$. 则 $G = \mathrm{Gal}(X^n - a)$ 是 n 阶群.

证明 设 $u^n - a = 0$. 则 $\prod_{\eta \in G} \eta(u) \in P$. 但 $\eta(u) = \zeta^{i(\eta)} u$, 而因为 1 的全部 n 次根都在 P 上, 所以 $\prod_{\eta \in G} \eta(u) = w u^{|G|} \in P \Longrightarrow u^{|G|} \in P$. 由此推出 $a = u^n = \left(u^{|G|}\right)^d$, 其中 $d = n/|G|$. 根据条件 (若命 $b = u^{|G|}$), 这只有当 $d = 1$ 时, 即 $|G| = n$ 时才是可能的. □

实际上我们证明了所有二项方程 $X^n - a = 0$ $(a \in P)$ 在 $\zeta \in P$ $(\zeta^n = 1, \zeta^m \neq 1, 0 < m < n)$ 的条件下, 其伽罗瓦群是循环群. 在相同的假定下, 上述断言的逆也成立. 下面两个定理中提到了更奥妙的情况.

定理 8 特征 $p > 0$ 的域 P 的每一个 p 维循环扩张 F 有形状 $F = P(c)$, 其中 $c^p - c \in P$.

证明 注意到 $1 \in P$ 及 $T_P^F(1) = [F:P] \cdot 1 = p \cdot 1 = 0$, 利用定理 6: 对某个 $c \in F$ 有 $\eta(c) = c + 1$. 在这种情形, $\eta^i(c) = c + i$, 即 $\langle \eta \rangle$-轨道 $\{c, c+1, \cdots, c+p-1\}$ 由 $p = [F:P]$ 个元素组成. 因此, $F = P(c)$. 此外,

$$\eta\left(c^p - c\right) = (\eta(c))^p - \eta(c) = (c+1)^p - (c+1) = c^p - c,$$

因此 $c^p - c \in P$. □

可以赋予这个定理以更精确的形式.

定理 9 (阿廷–施赖埃尔 (Schreier)) *设 P 是特征为 $p > 0$ 的域, 则下面的断言成立.*

1) 若 F/P 是 p 次循环扩张, 则 $F = P(c)$, 其中元素 c 满足方程 $X^p - X - a = 0$, 对某个 $a \in P$.

2) 反之, 对于给定的 $a \in P$, 多项式 $f(X) = X^p - X - a$ 或者在 P 中有一个根 (则其时它的全部根都在 P 中), 或者不可约. 在后一情形, $F = P(c)$ 是 P 上 p 次循环扩张, 对任意根 $c : f(c) = 0$.

证明 断言 1) 等价于定理 8.

反之, 若 $f(c) = 0$, 则 $f(c+i) = 0, i = 1, \cdots, p-1$, 即多项式 $f(X)$ 有 p 个不相同的根. 若根 $c \in P$, 则也有 $c + i \in P$. 现在假定 $c \notin P$, 并设 $f(X) = g(X)h(X), 1 \leqslant \deg g(X) < p$. 因为

$$f(X) = \prod_{i=0}^{p-1} (X - c - i),$$

所以 $g(X)$ 是某一部分线性因子的乘积. 设 $d = \deg g(X)$. X^{d-1} 前面的系数是

$-\sum_i'(c+i) = -dc+j$. 但是在 P 中 $d \neq 0$, 因此 $c \in P$, 这是因为 $g \in P[X]$, 矛盾.

因此, $f(X)$ 在 P 上不可约, 而它的全部根都在 $P(c)$ 中, 于是扩张 $P(c)$ 在 P 上是正规的. 因为 $f(X)$ 没有重根, 所以 $P(c)$ 是伽罗瓦扩张. 存在域 $P(c)$ 在 P 上的自同构 σ, 使 $\sigma(c)=c+1$. 像 $\sigma^i(c)=c+i\,(i=0,1,\cdots,p-1)$ 不相同, 于是伽罗瓦群由幂 σ^i 组成, 即是循环群. □

5. 方程可用根式解的判别法 我们将假定代数方程的系数在特征为 0 的域 P 中. 那么, 设 $f \in P[X]$.

定义 称扩张 F/P 是**根式扩张**, 如果它有一个子域塔

$$P = P_0 \subset P_1 \subset P_2 \subset \cdots \subset P_{r-1} \subset P_r = F, \tag{1}$$

其中

$$P_i = P_{i-1}(u_i), \quad u_i^{n_i} = a_i \in P_{i-1}, \quad 1 \leqslant i \leqslant r, \quad n_i \in \mathbb{N},$$

即 P_i 由添加某个根式 $\sqrt[n_i]{a_i}$ 于 P_{i-1} 得到.

也称方程 $f(X)=0$ 在 P 上**可用根式解**, 若存在 (1) 型的根式扩张, 它含有多项式 f 的全部根.

我们看到, F 含有正规扩张, 即含有分裂域, 但它本身未必是正规的. 这一缺陷是容易修正的.

定理 10 每一个根式扩张可被包含在某个正规的根式扩张中.

证明 我们对塔 (1) 的高度 r 用归纳法进行证明. 若 $r=1$ 且 $F=P(u), u^n=a \in P$, 而 ζ 是 1 的 n 次本原根, 则多项式 X^n-a 的分裂域 $P(\zeta,u)$ 恰好也将是正规的根式扩张.

假定扩张 $P_{r-1} \supset P$ 被包含在正规的根式扩张 $K \supset P$ 中, 且 $F=P_{r-1}(u), u^n=a \in P_{r-1}$, 我们考察元素 $a \in P_{r-1}$ 在 P 上的极小多项式 $h(X)$. 根据正规性的定义, 多项式 $h(X)$ 在域 K 上分解成线性因子的乘积:

$$h(X) = (X-a_1)(X-a_2)\cdots(X-a_m), \quad a_1 = a.$$

设 L 是多项式 $h(X^n)$ 在 P 上的分裂域. 因为正规扩张的交及合成恒是正规的, 所以合成 $K \cdot L = K(\zeta, u_1, \cdots, u_m)$ 也是正规的, 其中 $u_i^n = a_i$. □

下面的定理 11 几乎同样是显然的.

定理 11 正规根式扩张 F/P 的伽罗瓦群 $\mathrm{Gal}\,F/P$ 是可解群.

证明　不失一般性, 我们认为 F 是塔 (1) 确定的. 现在我们对域 F 添加 1 的一个

$$n = n_1 n_2 \cdots n_{r-1} n_r$$

次本原根 ζ, 并考察塔

$$P \subset P(\zeta) \subset P_1(\zeta) \subset \cdots \subset P_{r-1}(\zeta) \subset P_r(\zeta) = F(\zeta). \tag{2}$$

群 $\mathrm{Gal}\, P(\zeta)/P$ 是交换群, 而塔 (2) 中其余的一串扩张根据定理 7 是循环的. 基于伽罗瓦对应, 群 $G = \mathrm{Gal}\, F(\zeta)/P$ 有正规列

$$G \rhd G_0 \rhd G_1 \rhd \cdots \rhd G_{r-1} \rhd \{e\},$$

其中商群 G/G_0 是交换群, 而其余的一串商群 G_i/G_{i+1} 是循环群. 根据第 2 章 §2 中的定理 1, 群 G 应该是可解群. 若 $H = \mathrm{Gal}\, F(\zeta)/F$, 则 $H \lhd G$ (这是因为 F/P 是正规扩张), 从而 $\mathrm{Gal}\, F/P \cong G/H$ 也是可解群. □

最后, 我们来到 E. 伽罗瓦的 "顶尖级成就".

定理 12　*多项式方程 $f(x) = 0$ 可用根式解当且仅当群 $\mathrm{Gal}(f)$ 是可解群.*

证明　1) 假定多项式 $f(X)$ 的全部根 $\lambda_1, \cdots, \lambda_m$ (方程 $f(x) = 0$ 的零点) 都在正规根式扩张 F/P 中. 自然的包含

$$P \subset P(\lambda_1, \cdots, \lambda_m) \subset F$$

意味着方程 $f(x) = 0$ 的伽罗瓦群是可解 (根据定理 11) 群 $\mathrm{Gal}\, F/P$ 的商群. 因此它自己是可解群.

2) 设 F 是多项式 $f \in P[X]$ 的分裂域. 假定群 $G = \mathrm{Gal}\, F/P$ 是可解群且

$$G \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_{k-1} \rhd G_k = \{e\}$$

是它的合成列. 则正如我们知道的, 合成因子 G_i/G_{i+1} 将是素数阶循环群. 伽罗瓦对应又保证了存在子域链

$$P \subset F_1 \subset F_2 \subset \cdots \subset F_{k-1} \subset F_k = F,$$

其中每一个相继的扩张 F_{i+1}/F_i 将是素数次循环扩张.

我们对 F 添加一个 1 的 $n = |G|$ 次本原根 ζ, 并考察子域链

$$P \subset P(\zeta) \subset F_1(\zeta) \subset F_2(\zeta) \subset \cdots \subset F_{k-1}(\zeta) \subset F_k(\zeta) = F(\zeta).$$

每一个扩张 $F_{i+1}(\zeta)/F_i(\zeta)$ 也将是素数 p_i (整除 n) 次循环扩张. 根据定理 7, 域 $F_{i+1}(\zeta)$ 是对 $F_i(\zeta)$ 添加某个二项方程 $x^{p_i} - a = 0 (a \in F_i(\zeta))$ 的一个根得到的. 而这已意味着 $F(\zeta)$ 是域 P 的含有多项式 $f(X)$ 的全部根的根式扩张, 即多项式方程 $f(x) = 0$ 可用根式解. □

上面举出过任意次数的而其伽罗瓦群是对称群的标准多项式 $f\in\mathbb{Z}[X]$ 的例子. 根据刚刚证明了的定理 12, 相应的方程 $f(x)=0$ 不可用根式解.

现在我们假定多项式 $f\in P[X]\,(P\subset\mathbb{R})$ 的根都是实数. 对 P 添加实数根式的实数值是否就可以得到这些根? 我们使问题的提法更明确些.

定义 设 L 是多项式 $f\in P[X]$ 的分裂域, $P\subset L\subset\mathbb{R}$. 称方程 $f(x)=0$ **可用实根式解**, 若存在域 $F\,(P\subset L\subset F\subset\mathbb{R})$, 它有子域链

$$P=F_0\subset F_1\subset F_2\subset\cdots\subset F_{m-1}\subset F_m=F,\quad F_{i+1}=F_i\,(\sqrt[p_i]{a_i}),\tag{3}$$

其中 $a_i\in F_i$, 且 $\sqrt[p_i]{a_i}$ 是根式的实数值. 域 L 在这种情形叫做域 P 的**实根式扩张**.

定理 13 有限正规扩张 $L/P\,(P\subset L\subset\mathbb{R})$ 是实根式扩张当且仅当它的伽罗瓦群是 2-群.

证明 1) 任意有限 2-群 G 是可解群 (见第 2 章 §1 中的习题 2). 现在如果 $G=\operatorname{Gal}L/P$ 且

$$G=G_0\rhd G_1\rhd\cdots\rhd G_{n-1}\rhd G_n=\{e\}$$

是它的合成列, 则 $|G_i/G_{i+1}|=2$. 伽罗瓦对应给出子域链

$$P=L_0\subset L_1\subset L_2\subset\cdots\subset L_{n-1}\subset L_n=L\tag{4}$$

其中, 一串扩张

$$L_{i+1}=L_i\,(\sqrt{a_i}),\quad a_i\in L_i$$

都是 2 次循环扩张. 这已经意味着 L/P 是实根式扩张.

2) 现在我们将从正规实根式扩张 $L/P\,(P\subset L\subset F\subset\mathbb{R})$ 出发, 其中域 F 有形如 (3) 的子域链, 且其中的 p_i 是素数.

伽罗瓦群 $G=\operatorname{Gal}L/P$ 是可解群, 因此, 在对应于群 G 的某个合成列的形如 (4) 的子域链中, 一串扩张 L_{i+1}/L_i 将都是素数次循环扩张. 不失一般性, 可以认为 L/P 是素数 q 次循环扩张, 且 $L\not\subset F_{m-1}$ (在相反的情形可以用 F_{m-1} 代替 F). 则合成 $L\cdot F_{m-1}$ 是 F_{m-1} 上 q 次循环扩张. 用 F_{m-1} 代替 P, 并用 $L\cdot F_{m-1}$ 代替 L (然后回到原来的记号), 我们将问题简化为

$$P\subset L\subset P\,(\sqrt[p]{a})\subset\mathbb{R},\quad a\in P,$$

且 L/P 是素数 q 次循环扩张的情形. 所指的是, $\sqrt[p]{a}$ 是素数 p 次根式的实数值. 在所考察的情形, 多项式 X^p-a 的根中没有一个在域 $P(\subset\mathbb{R})$ 中, 但是已知 (见 §3 中的习题 1) 在域 P 中没有根的多项式 X^p-a 在 $P(\zeta)$ 上是不可约的 $(\zeta^p=1)$. 于是 $[P\,(\sqrt[p]{a}):P]=p$, 这只有当 $q=p$ 时才是可能的. 于是 $L=P\,(\sqrt[p]{a})$ 是伽罗瓦扩张. 在这种情形, 不可约多项式 $X^p-a\in P[x]$ 在 $P\,(\sqrt[p]{a})\subset\mathbb{R}$ 中分解成线性因式的乘积. 因为当 p 是奇数时, 多项式的根不全都是实数, 所以得到结论: $p=2$. □

习　题

1. 方程

$$x^6+2x^5-5x^4+9x^3-5x^2+2x+1=0$$

是否可用根式解?

2. 设 ζ 是 1 的 5 次本原根, $a,b\in\mathbb{Q},\alpha_i$ 是方程

$$x^5-5ax^3+5a^2x-2b=0$$

的零点. 证明:

$$\alpha_i=\zeta^i\sqrt[5]{b+\sqrt{b^2-a^5}}+\zeta^{5-i}\sqrt[5]{b-\sqrt{b^2-a^5}},\quad 0\leqslant i\leqslant 4.$$

3. 证明: 若域 $P(\subset\mathbb{R})$ 上不可约多项式 X^3+px+q 的三个根全都是实数, 则这三个根不可能用实根式表出.

4. 利用元素 u 的拉格朗日预解式 $\mathcal{L}(u)$ 可以证明 §3 ~ §4 中的一系列断言. 即如果 $F=P(u)$ 是域 P 的含有 1 的 n 次本原根 ζ 的 n 次循环扩张, 并且如果 $\mathrm{Gal}\,F/P=\langle\sigma\rangle,v\in F$, 则根据定义

$$\mathcal{L}(v)=v+\zeta^{-1}\sigma(v)+\zeta^{-2}\sigma^2(v)+\cdots+\zeta^{-(n-1)}\sigma^{n-1}(v).$$

验证: 拉格朗日预解式有以下性质:

a) $\sigma(\mathcal{L}(v))=\zeta\mathcal{L}(v)$;

b) $\mathcal{L}(v)^n\in P$;

c) 存在元素 $v\in F$ 使 $\mathcal{L}(v)\neq 0$.

§6 有限群中的刚性和有理性

在本节中伽罗瓦理论直接和特征标理论结合起来. 叙述上的概略性将用指出相应的文献来弥补.

1. 定义及基本定理的表述　设 G 是有单位元 e 的有限群. 我们在 G 中取定某些共轭类 $\mathcal{K}_1,\cdots,\mathcal{K}_m$, 并命

$$\widetilde{\mathcal{S}}=\widetilde{\mathcal{S}}(\mathcal{K}_1,\cdots,\mathcal{K}_m)=\{(g_1,\cdots,g_m)|g_i\in\mathcal{K}_i,g_1g_2\cdots g_m=e\}.$$

我们在 $\widetilde{\mathcal{S}}$ 中分出一个子集

$$\mathcal{S}=\mathcal{S}(\mathcal{K}_1,\cdots,\mathcal{K}_m)=\left\{(g_1,\cdots,g_m)\in\widetilde{\mathcal{S}}|\langle g_1,\cdots,g_m\rangle=G\right\}.$$

显然, G 通过共轭作用在 $\widetilde{\mathcal{S}}$ 上, 也作用在 $\mathcal{S}$ 上. 更进一步, 我们认为 $Z(G)=e$. 在这种情形, G 在 $\mathcal{S}$ 上的作用是自由的. 事实上, 若 $g\in G$ 使 $(g_1,\cdots,g_m)$ 不动, 则 g 与所有的 g_i 可交换, 从而与 G 中所有元素可交换, 这是因为 $\langle g_1,\cdots,g_m\rangle=G$. 然而这时 $g=e$, 这是由于 $Z(G)=e$.

定义 称共轭类组 $(\mathcal{K}_1, \cdots, \mathcal{K}_m)$ 是**刚性的**, 若 $\mathcal{S}(\mathcal{K}_1, \cdots, \mathcal{K}_m) \neq \varnothing$ 且 G 传递地作用在 $\mathcal{S}$ 上, 即由于作用是自由的, $|\mathcal{S}| = |G|$.

组 $(\mathcal{K}_1, \cdots, \mathcal{K}_m)$ 叫做**强刚性的**, 若它是刚性的且 $\mathcal{S} = \widetilde{\mathcal{S}}$ (一般说, $\mathcal{S} \subset \widetilde{\mathcal{S}}$).

因此, 若 $|\widetilde{\mathcal{S}}| = |\mathcal{S}| = |G|$, 则强刚性成立. 现在我们看到

$$|\widetilde{\mathcal{S}}| = N(\mathcal{K}_1, \cdots, \mathcal{K}_m) \tag{1}$$

等于方程

$$g_1 g_2 \cdots g_m = e, \quad g_i \in \mathcal{K}_i$$

的解 $(g_1^0, \cdots, g_m^0)$ 的个数.

现在设 $\mathrm{Cl}(G) = \{\mathcal{K}_1, \cdots, \mathcal{K}_r\}$ 是有限群 G 的所有共轭类组成的集合, 而 n 是它的指数, 即群 G 的所有元素的阶的最大公因子. 群 $U(Z_n)$ 作用在 G 上: $g \mapsto g^s, \bar{s} \in U(Z_n)$, 并且类似地作用在 $\mathrm{Cl}(G)$ 上. 进一步, $\mathrm{Irr}(G) = \{\chi_1, \chi_2, \cdots, \chi_r\}$ 是群 G 的不可约复特征标的集合. 我们知道, 值 $\chi_i(g)$ 在分圆域 $\Gamma_n = \mathbb{Q}(\zeta)$ $(\zeta^n = 1)$ 中. 因此, 存在着群 $\mathrm{Gal}\,\Gamma_n/\mathbb{Q} \cong U(Z_n)$ 在 $\mathrm{Irr}(G)$ 上的自然作用. $U(Z_n)$ 在 $\mathrm{Cl}(G)$ 上的作用和在 $\mathrm{Irr}(G)$ 上的作用由公式

$$\sigma_s(\chi)(g) = \chi(g^s)$$

相联系, 其中, 像通常情况一样, $\sigma_s(\zeta) = \zeta^s$.

定义 类 $\mathcal{K} \in \mathrm{Cl}(G)$ 叫做 $\mathbb{Q}$–**有理的** (或简称**有理的**), 若下面等价的性质成立:

1) 在 $U(Z_n)$ 的作用下, $\mathcal{K}$ 不动;

2) 每一个特征标 $\chi \in \mathrm{Irr}(G)$ 在 $\mathcal{K}$ 上所取的值在 $\mathbb{Q}$ 中 (实际上在 $\mathbb{Z}$ 中).

群 G 的共轭类组 $\{\mathcal{K}_i | 1 \leqslant i \leqslant m\}$ 是有理的, 若类中每一个 $\mathcal{K}_i$ 是有理的.

有理性条件表明, 若 $g \in \mathcal{K}$, 则循环群 $\langle g \rangle$ 的所有生成元都在 $\mathcal{K}$ 中, 即都与 g 共轭. 例如, 在对称群 S_n 中, 每一个共轭类都是有理的.

更一般地, 设 F 是任意域, $\mathcal{K} = g^G, \mathrm{g.c.d}(|\langle g \rangle|, \mathrm{char}\,F) = 1$. 若 $\chi(g) \in F, \forall \chi \in \mathrm{Irr}(G)$, 或者等价地, 若 $\mathcal{K}^n = \mathcal{K} \forall n$, 其中 $\sigma_n \in \mathrm{Gal}\,F(\zeta)/F$, 则称 $\mathcal{K}$ 是 F–有理的.

例 1 交错群 A_5 有阶为 $1, 2, 3, 5, 5$ 的五个共轭元素类. 设 $5A, 5B$ 是两个阶为 5 的共轭类. 若 $a \in 5A$, 则 $a^{-1} \in 5A$ 而 $a^2, a^3 \in 5B$, 因此 $5A, 5B$ 不是 $\mathbb{Q}$–有理的. 我们看到

$$\chi(5A), \chi(5B) \in \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\zeta), \quad \zeta^5 = 1.$$

有限群 G 的共轭类组 $\{\mathcal{K}_1, \cdots, \mathcal{K}_m\}$ 的强刚性及 $\mathbb{Q}$–有理性概念的重要性可用下面的基本定理来说明. 这个定理我们权且接受下来, 但不作证明.

定理 1 (别里 (Г. В. Белый)–汤普森 (J. Thompson)) 设 G 是有平凡中心的有限群, 并有有理的强刚性组, 则对某个伽罗瓦扩张 $F/\mathbb{Q}$, 我们有 $G \cong \mathrm{Gal}\,F/\mathbb{Q}$.

如果没有有理性, 则定理中的 $\mathbb{Q}$ 用扩张

$$L=\mathbb{Q}(\mathrm{Irr}(G))=\mathbb{Q}(\chi(g),\forall\chi\in\mathrm{Irr}(G);\quad g\in\mathcal{K}_1,\cdots,\mathcal{K}_m)=\mathbb{Q}(\zeta)$$

代替.

当群接近于单群, 且其共轭类组 $\{\mathcal{K}_1,\cdots,\mathcal{K}_m\}$ 是强刚性的, 在所有这些已知的情况下, $m=3$. 显然, 在这种情形, G 是有两个生成元的群. 定理 1 解决了现实的任务: 用特征标理论的语言表述出强刚性的性质, 即找出数 $N(\mathcal{K}_1,\cdots,\mathcal{K}_m)$ 的明显表达公式. 这个公式我们即将给出, 其后, 我们也将考察例子.

2. 解的计算 作群上的平均并利用舒尔引理 (第 3 章 §4) 就得到

$$\frac{1}{|G|}\sum_{t\in G}\Psi(txt^{-1})=\frac{\chi(x)}{\chi(e)}E$$

($\chi=\chi_\Psi$ 是群 G 的不可约表示 Ψ 的特征标). 用 $\Psi(y)$ 从右边来乘这个关系式并转移到迹, 我们得到

$$\frac{1}{|G|}\sum_{t\in G}\chi(txt^{-1}y)=\frac{\chi(x)\chi(y)}{\chi(e)}$$

类似地,

$$\frac{1}{|G|}\sum_{t_1\in G}\Psi\left(t_1x_1t_1^{-1}t_2x_2t_2^{-1}y\right)=\frac{\chi(x_1)}{\chi(e)}\Psi\left(t_2x_2t_2^{-1}y\right),$$

$$\frac{1}{|G|^2}\sum_{t_1,t_2\in G}\Psi\left(t_1x_1t_1^{-1}t_2x_2t_2^{-1}y\right)=\frac{\chi(x_1)}{\chi(e)}\frac{1}{|G|}\sum_{t_2\in G}\Psi\left(t_2x_2t_2^{-1}y\right)=\frac{\chi(x_1)\chi(x_2)}{\chi(e)^2}\chi(y).$$

对 n 的明显的归纳给出

$$\frac{1}{|G|^m}\sum_{t_1,\cdots,t_m}\chi\left(t_1x_1t_1^{-1}\cdots t_mx_mt_m^{-1}y\right)=\frac{\chi(x_1)\cdots\chi(x_m)}{\chi(e)^m}\chi(y).\tag{2}$$

现在设 φ 是 G 上任意的中心函数 (类函数), 则

$$\varphi=\sum_\chi c_\chi\cdot\chi,\quad c_\chi=(\varphi,\psi)_G.$$

利用 (2), 我们引入量

$$\begin{aligned}I_m(\varphi)&=\frac{1}{|G|^m}\sum_{t_1,\cdots,t_m}\varphi\left(\left(\prod_{i=1}^m t_ix_it_i^{-1}\right)y\right)\\&=\frac{1}{|G|^m}\sum_\chi\sum_{t_1,\cdots,t_m}c_\chi\chi\left(\left(\prod_{i=1}^m t_ix_it_i^{-1}\right)y\right)=\sum_\chi c_\chi\frac{\prod\limits_1^m\chi(x_i)}{\chi(e)^m}\chi(y).\end{aligned}\tag{3}$$

在 $\varphi=\delta$ 是狄拉克函数 ($\delta(e)=1$ 且 $\delta(g)=0, \forall g\neq e$) 的情形, 我们来估计 $I_m(\varphi)$. 显然

$$\delta=\frac{1}{|G|}\sum_{\chi}\chi(e)\chi$$

($1/|G|$ 乘上正则表示的特征标以后的值). 于是 $c_\chi=\chi(e)/|G|$. 若 $x_1,\cdots,x_m,y$ 是群 G 中给定的元素, 则

$$I_m(\delta)=\frac{1}{|G|^m}N'_m,$$

其中 $N'_m=N(x_1,\cdots,x_m,y)$ 是方程

$$t_1x_1t_1^{-1}\cdots t_mx_mt_m^{-1}y=e$$

的解 $(t_1,\cdots,t_m)$ 的个数. 因此, 借助 (3), 我们得到

$$\begin{aligned}N'_m=|G|^mI_m(\delta)&=|G|^m\sum_{\chi}\frac{\chi(e)}{|G|}\frac{\chi(x_1)\cdots\chi(x_m)\chi(y)}{\chi(e)^m}\\&=|G|^{m-1}\sum_{\chi}\frac{\chi(x_1)\cdots\chi(x_m)\chi(y)}{\chi(e)^{m-1}}.\end{aligned}$$

命 $y=e$, 我们得到公式

$$N_m=N(x_1,\cdots,x_{m-1},x_m)=|G|^{m-1}\sum_{\chi}\frac{\chi(x_1)\cdots\chi(x_m)}{\chi(e)^{m-1}}. \tag{4}$$

设 $\mathcal{K}_1,\cdots,\mathcal{K}_m$ 是具有代表 $x_1,\cdots,x_m$ 的共轭类, 并设 c_i 是 $\mathcal{K}_i$ 中元素的中心化子的阶, 则回想起 (1), 我们得到表达式

$$N(\mathcal{K}_1,\cdots,\mathcal{K}_m)=\frac{N_m}{c_1\cdots c_m}.$$

应用公式 (4) 并注意到 $c_i=|G|/|\mathcal{K}_i|$, 我们得到下面的断言.

定理 2 数 $N(\mathcal{K}_1,\cdots,\mathcal{K}_m)$ 由公式

$$N(\mathcal{K}_1,\cdots,\mathcal{K}_m)=\frac{1}{|G|}|\mathcal{K}_1|\cdots|\mathcal{K}_m|\sum_{\chi}\frac{\chi(x_1)\cdots\chi(x_m)}{\chi(e)^{m-2}} \tag{5}$$

确定, 其中 $\mathcal{K}_i=x_i^G$ 且 $\chi\in\mathrm{Irr}(G)$. □

最后这个定理有各种各样的用途. 例如, 可以用它来计算 G 中和交错群 A_5 同构的子群的个数. 事实上,

$$A_5=\langle x,y,z|x^2=y^3=z^5=e\rangle.$$

问题归结为找出方程 $xyz=e$ 的解的个数, 其中 x,y,z 相应地属于指数为 2,3 和 5 的共轭类. 同样的做法也可被应用于有类似的给定的生成元和关系式的 S_4,A_4,D_n.

刚性常常通过两个阶段来检验.

1. 根据群 G 的特征标表及公式 (5) 计算 $|\widetilde{\mathcal{S}}|$.

2. 通过求出 $\widetilde{\mathcal{S}}$ 中所有不生成 G 的 m 元组 $\{g_1,\cdots,g_m\}$ 计算 $|\widetilde{\mathcal{S}}-\mathcal{S}|=|\widetilde{\mathcal{S}}|-|\mathcal{S}|$; 为此利用关于群 G 的极大子群的知识.

命题 1 *下面的恒等式成立:*

i) $|\widetilde{\mathcal{S}}(\mathcal{K}_1^n,\cdots,\mathcal{K}_m^n)|=|\widetilde{\mathcal{S}}(\mathcal{K}_1,\cdots,\mathcal{K}_m)|,\quad \overline{n}\in U(Z_n)$;

ii) $|\mathcal{S}(\mathcal{K}_1^n,\cdots,\mathcal{K}_m^n)|=|\mathcal{S}(\mathcal{K}_1,\cdots,\mathcal{K}_m)|,\quad \overline{n}\in U(Z_n)$.

证明 第一个恒等式由公式 (5) 并结合公式 $\chi(g^n)=\sigma_n(\chi)(g)$ 推出.

第二个等式按以下方式对阶 $|G|$ 用归纳法证明. 对任意子群 $H\subset G$, 我们命

$$\mathcal{S}^{(H)}(\mathcal{K}_1\cap H,\cdots,\mathcal{K}_m\cap H)=\{(g_1,\cdots,g_m)|g_i\in\mathcal{K}_i\cap H, g_1\cdots g_m=e,\langle g_1,\cdots,g_m\rangle=H\}.$$

一般说, $\mathcal{K}_i\cap H$ 不是 H 中单独一个共轭类, 而是几个这种类的并集. 公式

$$\widetilde{\mathcal{S}}-\mathcal{S}(\mathcal{K}_1,\cdots,\mathcal{K}_m)=\bigcup_{H\subset G,H\neq G}\mathcal{S}^{(H)}(\mathcal{K}_1\cap H,\cdots,\mathcal{K}_m\cap H)$$

用来达到归纳证明. □

3. 刚性的例子 a) *对称群* S_n. 显然 $S_n(n\geqslant 3)$ 含有对应于长度为 $n,2,n-1$ 的循环置换的共轭类 $nA,2A,\mathcal{K}$. 我们来证实三元组 $(nA,2A,\mathcal{K})$ 是强刚性的.

事实上, 给定的 n-循环置换 $x\in nA$ 给出集合 $\{1,2,\cdots,n\}$ 的一个循环排序, 即一个定向的 n 边形. 这个 n 阶置换和一个对换的合成恰好给出一个 $(n-1)$-循环置换当且仅当两个被置换的顶点并列 (紧靠在一起). 于是, 具有阶为 $n,2,n-1$ 的循环置换 x,y,z 的方程 $xyz=e$ 的解与具有一个标出边的定向 n 边形是一一对应的. 任意两个这样的构形可以通过 S_n 中的一个置换将一个变为另一个. 因此, $|\widetilde{\mathcal{S}}|=|G|=n!$ 照样也有 $\widetilde{\mathcal{S}}=\mathcal{S}$, 这是因为 $\langle x,y,z\rangle=S_n$. 正如已经看出的, 在 S_n 中每一个共轭类都是有理的. 因此, 根据定理 1, 存在伽罗瓦扩张 $F/\mathbb{Q}$ 使 $\operatorname{Gal}F/\mathbb{Q}\cong S_n$. 当然, 对我们来说, 这不是新鲜的东西 (见 §4), 而只不过是新方法的一个例证.

b) *群* $\mathrm{PSL}(2,\mathbb{F}_p)$. 当 $p>3$ 时, 这个群是单群 (见第 2 章 §2 中的定理 4). 它的所有复特征标都是已知的, 但是我们只限于讨论 $\mathrm{PSL}(2,\mathbb{F}_p)$ 包含阶为 2 和 3 的共轭元素类 $2A$ 和 $3A$ 中的至少一个. 阶为 p 的元素类有两个: pA,pB, 它们有代表元: 幂单矩阵 $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ 和 $\begin{pmatrix}1&\alpha\\0&1\end{pmatrix}$, 其中勒让德记号 $\left(\dfrac{\alpha}{p}\right)=-1$. 当 $\left(\dfrac{2}{p}\right)=-1$ 时, 三元组 $(2A,3A,pA)$ 和三元组 $(2A,pA,pB)$ 的强刚性以及当 $\left(\dfrac{3}{p}\right)=-1$ 时, 三元组 $(3A,pA,pB)$ 的强刚性可直接验得. 这里, 正如以前考察过的群 $A_5\cong\mathrm{PSL}(2,5):=\mathrm{PSL}(2,\mathbb{F}_5)$ 的例子所指出的, 一般说来不能指望有有理性.

c) *阶为* $504=2^3\cdot 3^2\cdot 7$ *的单群* $\mathrm{SL}(2,8)=\mathrm{SL}(2,\mathbb{F}_8)$. 构造它的不可约复特征标表是一个很好的习题:

·	$1A$	$2A$	$3A$	$7A$	$7B$	$7C$	$9A$	$9B$	$9C$
χ_1	1	1	1	1	1	1	1	1	1
χ_2	7	-1	-2	0	0	0	1	1	1
χ_3	7	-1	1	0	0	0	α	α'	α''
χ_4	7	-1	1	0	0	0	α''	α	α'
χ_5	7	-1	1	0	0	0	α'	α''	α
χ_6	8	0	-1	1	1	1	-1	-1	-1
χ_7	9	1	0	β	β'	β''	0	0	0
χ_8	9	1	0	β''	β	β'	0	0	0
χ_9	9	1	0	β'	β''	β	0	0	0

这里

$$\alpha = -2\cos\frac{2\pi}{9}, \quad \alpha' = -2\cos\frac{4\pi}{9}, \quad \alpha'' = -2\cos\frac{8\pi}{9},$$
$$\beta = 2\cos\frac{2\pi}{7}, \quad \beta' = 2\cos\frac{4\pi}{7}, \quad \beta'' = 2\cos\frac{8\pi}{7}.$$

根据公式 (5), 我们有

$$|\widetilde{S}(9A, 9B, 9C)| = \frac{504^2}{9^3}\left(1 + \frac{1}{7} + \frac{1}{7} + \frac{1}{7} + \frac{1}{7} - \frac{1}{8} + 0 + 0 + 0\right) = 504 = \mathrm{SL}(2, 8).$$

为了确信有刚性, 只要证实任意三元组 $(x, y, z) \in \widetilde{S}$ 生成 $\mathrm{SL}(2, 8)$. 我们取定域

$$\mathbb{F}_8 = \left\{0, 1, \lambda^i | 1 \leqslant i \leqslant b\right\}, \quad \lambda^3 = \lambda + 1.$$

应该记住 $\mathbb{F}_8$ 是特征为 2 的域且 $\mathbb{F}_8^* = \langle\lambda\rangle$. 我们取矩阵

$$a = \begin{pmatrix} \lambda^2 + 1 & \lambda + 1 \\ \lambda + 1 & \lambda + 1 \end{pmatrix}, \quad b = \begin{pmatrix} \lambda^2 + \lambda + 1 & \lambda \\ \lambda + 1 & 1 \end{pmatrix}, \quad c = \begin{pmatrix} \lambda^2 & \lambda \\ \lambda^2 + \lambda + 1 & 1 \end{pmatrix}$$

作为三元组中的元素. 容易验证 $a^9 = b^9 = c^9 = e, abc = e$, 矩阵 $d = a^4b^2 = \mathrm{diag}(\lambda^{-1}, \lambda)$ 的幂穷尽了群 $\mathrm{SL}(2, 8)$ 的所有对角线元素. 更进一步, 得到幂单矩阵

$$u = a^2b^4a^4b^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \overline{u} = a^{-2}d^{-1}a^2b^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

且此后立即得到在布吕阿分解 (见第 2 章 §1 中定理 4 的证明) 中起着关键作用的元素 $w = u\overline{u}u = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. 剩下的只要得到标准博雷尔子群. 但是我们略去计算中的细节.

习　题

1. 设 G, H 是有限群, 有强刚性的共轭类组

$$\widetilde{S}(\mathcal{K}_1, \cdots, \mathcal{K}_m), \quad \widetilde{S}\left(\mathcal{K}'_1, \cdots, \mathcal{K}'_{m'}\right)$$

证明: 这时

$$\widetilde{\mathcal{S}}\left(\mathcal{K}_i \times \mathcal{K}'_j \,\middle|\, 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant m'\right)$$

是 $G \times H$ 中强刚性共轭类组.

2. 设 σ 是有限群的外自同构, 并设 $(\mathcal{K}_1, \cdots, \mathcal{K}_m)$ 是 G 中刚性共轭类组. 证明: 这时存在 i 使 $\sigma(\mathcal{K}_i) \neq \mathcal{K}_i$.

3. 我们已经知道交错群 A_5 有共轭类 $1A, 2A, 3A, 5A, 5B$. 证明: 三元组

$$(2A, 3A, 5A), \quad (2A, 5A, 5B), \quad (3A, 5A, 5B)$$

都是强刚性的. 由此推出 $A_5 \cong \mathrm{Gal}\, F/\mathbb{Q}(\sqrt{5})$

4. 我们用 $K_1(z)$ 来记有限群 G 中元素 z 表示成换位子形状的表示的个数, 即方程 $z = xyx^{-1}y^{-1}$ 的解的个数. 证明:

$$K_1(z) = |G| \sum_{i=1}^{r} \frac{\chi_i(z)}{\chi_i(e)}.$$

更一般地, 若 $K_m(z)$ 是方程

$$z = \left(x_1 y_1 x_1^{-1} y_1^{-1}\right)\left(x_2 y_2 x_2^{-1} y_2^{-1}\right) \cdots \left(x_m y_m x_m^{-1} y_m^{-1}\right)$$

的解的个数, 则

$$K_m(z) = |G|^{2m-1} \sum_{i} \frac{\chi_i(z)}{\chi_i(e)^{2m-1}}.$$

§7 结束语

2011 年 11 月 7 日是 19 世纪最著名的数学家 E. 伽罗瓦 (1811—1832) 诞生 200 周年的日子. 时至今日, 伽罗瓦的思想已渗透到数学的各个不同领域, 就连通常称之为伽罗瓦经典理论的东西, 也以它自己的创新继续令人感到惊讶. 在伽罗瓦以前所得到的关于代数方程的零散的事实被他合并起来并用群论的方法作出了极大的发展, 虽然群论这个理论在当时还不存在. 当时只有单个的群的例子及单个的最简单的概念 (拉格朗日, 高斯, 柯西, 阿贝尔等都提及过), 甚至连任何一种统一的术语也没有. 伽罗瓦所引入的**可解群**, **单群**, **正规子群**等概念直到现在仍是一般群论中最常使用的. 不可改变的发展逻辑将伽罗瓦引向有限域 (伽罗瓦域, 高斯曾局部地涉及过) 和有限域上分式线性变换群. 他证明了 $n \geqslant 5$ 时 A_n (交错群) 的单性和 $q \geqslant 4$ 时 $\mathrm{PSL}(2, q)$ 的单性. 伽罗瓦关于本原置换群、素数阶可迁置换群和作为可迁置换群的 $\mathrm{PSL}(2, q)$ 的表示的次数的定理可以认为是一个半世纪以后得到的一般分类结果的典范. 用群论语言表述出的素数次代数方程 (系数是有理整数) 可用根式解的条件以其完备性和优美性而显示出它的出众. 而所有这些都是 E. 伽罗瓦在 16 岁到 21 岁这一年龄段深入细致地思考和证明的. 在数学中作出了不可估量的贡献的 H. Weyl 说

(见 [8]): “数十年来, 这本经过七次出版的手稿中留下来的伽罗瓦的思想, 后来对整个数学的发展产生越来越深远的影响. 这些思想包含在伽罗瓦于一场有点傻的决斗中丧生的前一天写给友人的告别信中, 其时他还不到 21 岁. 根据在这封信中所表达出的思想的新意和深远性, 这封信可能是人们手写作品中最杰出的一件. 在 L. Infeld [13] 中, 作者以浓重的笔墨动情地记述了伽罗瓦短促的谜一样的一生.

F. 克莱因也在其卓越的史论性著作 [15] 中对伽罗瓦在数学中的贡献作出了总的估价. 特别地, 克莱因写道: “不了解 ‘伽罗瓦理论’ 就难于估计出他的成就的全部意义. 因此, 我希望尝试着用几句话来描绘出这一理论的基本构思, 虽然在如此简短的叙述中不可能给出它的全貌. 在做这件事以前, 我首先想指出伽罗瓦理论作为我们大学中一门课程所起的独特作用. 这里有一个使教和学双方同样感到惋惜的矛盾. 一方面, 为这一极富独创的发明及其深邃结果的重要性所鼓舞, 广大教师特别乐于讲授伽罗瓦理论这门课, 但另一方面, 开始学习的大学生又恰恰特别难于理解这一方面的内容. 在大多数情况下, 令人痛惜的结果是, 教师注入了爱、付出了努力, 但除极少数例外, 大多数听课的人却毫无所获. 伽罗瓦理论在叙述上的特殊困难在这一方面也起了一定作用.”

上面所说的关于伽罗瓦理论的特殊地位的见解是根深蒂固的, 它引起了数论大师 A. Weil 的注意. 他在为其自己的书的俄译本所作的序言中写道: “曾经有过一段时间, 伽罗瓦理论被当作是难懂的、抽象的东西, 只是为一些专家们写的. 不仅如此, 我还知道一些和我同时代的卓越的数学家, 他们公开承认他们对伽罗瓦理论一无所知, 并且似乎甚至还以此为荣. 现在, 大家都已充分认识到这是一个基本的分支, 每一个严肃认真的数学专业大学生应该在头几年的教育中就了解它”.

近年来, 伽罗瓦理论的逆问题引起了极大的注意, 要得到它的令人满意的解答 (暂时还没有), 需要深入数论、代数几何, 自然还有群论, 包括表示论在内. 看来, 克莱因所描述的情况只不过更严重罢了. 同时, 如果大学生一开始就把注意力集中于伽罗瓦理论的基本原理, 这种理论不过分拘泥于技巧, 但会大大提高他们的水平并能得到有意思的结果, 那么, 对于这些大学生来说, 处于许多门数学学科交接处的这门科目应该是极其诱人的. 第 5 章中的论述就是致力于这一目标的. 伽罗瓦理论正问题 (对于任意多项式 $f \in \mathbb{Q}[X]$, 计算群 $\mathrm{Gal}(f)$) 和逆问题 (构造有给定伽罗瓦群的多项式) 还将长期成为一个严肃的研究课题, 更不用说, 在更加完整的意义下, 伽罗瓦理论对整个数学都具有意义了.

附录　未解决的问题

1. 有限单群的分类　实际上, 这个经典问题被认为已经解决. 其答案是: 每个有限单群 (自然地, 指非素数阶循环群) 同构于下列群之一: 交错群, 李型群, 散在群. 我们不讲任何定义, 以免陷入细节. 散在单群有 26 个. 其中有我们在第 2 章序言中谈到的 "大得出奇的 M" (为了纪念最早发现者 Norton-Fischer, 有另一个记号 $M = F_1$). D. Gorenstein 在《有限单群——单群分类引论》一书中对总的情况给予了很好的描写 (M: Мир 1985). 答应给出的数千页的证明至今还没有出示, 但该方面工作仍在积极进行. 如果连这么严重的缺陷都发现不了, 那么这个证明对于广大的数学工作者来说是不能接受的. 再次想说的是, 数学的力量在于它的统一性, 谁又能知道, 对于这些经多年努力而得出的结论用什么途径和什么方法才能够给出令人信服的和容易验证的论据.

关于任意奇阶群的可解性的著名的 J. Thompson 和 W. Feit 定理 (1962) 确定了有限单群研究的一般方向. 其证明长达杂志的 255 页. 在其后的一些数学家的著作中, 这个证明变得更加简洁 (如 Bender H, Glauberman G, Local Analysis for the Odd Order Theorem, Cambridge Univ. Press, 1994), 但是, 尽管如此, 也没有缩短到 100 页之内. 这个问题的一个简单的重新表达方式是下面这种形式: 假设在所给类中存在一个非可解群, 那么我们应该得到一个等于自己换位子群的奇阶群 G. 但是如果 $G = G'$, 那么由第 4 章 §4 定理 7 的推论, 有关系:

$$|G|\prod_{i=1}^{r}\mathcal{K}_i = \left(\prod_{i=1}^{r}|\mathcal{K}_i|\right)\sum_{j=1}^{r}\mathcal{K}_j. \qquad (*)$$

借助于特征标理论得到的关系 $(*)$, 在群是奇阶的情况下可以按模 2 简化且在特征

为 2 的域上考虑, 这时它还具有更漂亮的形式:

$$\prod_{i=1}^{r} \mathcal{K}_i = \sum_{j=1}^{r} \mathcal{K}_j \qquad (**)$$

"仅仅" 需要证明, 关系 (*), (**) 实际上对子奇阶群永远都不可能成立. 要做到这一点仅仅用一个特征标理论的方法是不可能的.

2. 正则自同构 正如在 [BA I] 第 4 章 §2 所见到的, 群 Aut(G) 和甚至一个元 $\varphi \in \mathrm{Aut}(G)$ 可以作为群 G 的重要信息来源. 如果

$$a \neq e \Longrightarrow \varphi(a) \neq a,$$

则 φ 称为**正则自同构**. J. Thompson 关于具有素数 p 阶的正则自同构的群 G 的幂零性的重要定理导致了大量结果并刺激了人们研究群 G 的幂零类 n 的可能量的兴趣. 当 $p=2$ 时, 群 G 是交换群, 而在一般情况下被证明 (А. Кострикин, В. Крекнин) $n = n(p) < p^p$. 而 G. Higman 猜想, 是:

$$n(p) = \frac{(p^2-1)}{4}.$$

当 $p = 3, 5$ 时, 这个猜想是正确的, 且随着计算机算出的结果, 似乎当 $p = 7$ 时也正确. 要是能够证明这个算出的结果和改善一般的估计就好了. 另一个关于具有任意阶的正则自同构的有限群的可解性的猜想更为重要得多. 对于它的证明的直接方法暂时还没有.

3. 奇异李代数 是否存在无限维的李代数, 其所有真子代数是一维的? 如果存在, 那么这意味着 L 由任意两个不成比例的元生成

$$\dim\langle a, b\rangle_F = 2 \Longrightarrow L = \mathrm{Lie}(a, b).$$

域 F 可以认为是任意的, 比如说, 可以是 $\mathbb{C}$. 在群论中这种奇异李代数的类似物是存在的: А. Ю. Ольшанский 曾构造了无限 p–群, 其所有真子群为 p 阶循环群 (素数 p 假定足够大).

4. 伯恩赛德 (Burnside) 问题 假设 $F_2 = Gr(x, y)$ 是一个具有两个生成元 x, y 的自由群, 且设 F_2^n 是所有元素 $w \in F_2$ 的 n 次幂 w^n 生成的正规子群. 问 "自由的" Burnside 群 $B(n) = F_2/F_2^n$ 是有限的还是无限的? 对于 $n = 2, 3, 4, 6$ 回答是肯定的, 对于所有足够大的 n 回答是否定的. 不知道答案的最小数是 $n = 5$. 部分的重新表达归结如下.

令:

$$(x, y; 1) := (x, y) = xyx^{-1}y^{-1},$$
$$(x, y; s+1) := ((x, y; s), y).$$

是否找到那样的元 $w_i(x,y)$ 和整数 m, 使得在 F_2 中有下列关系

$$(x,y;6)=\prod_{i=1}^{m} w_i(x,y)^5?$$

如果不是, 那 Burnside 群 $B(5)$ 是无限的; 如果是, 那么 $B(5)$ 将具有漂亮的恩格尔性质.

为便于理解, 我们回想一下

$$(x,y;1)=(xy)^2\left(y^{-1}x^{-1}y\right)^2\left(y^{-1}\right)^2,$$
$$(x,y;2)=\left(xyx^{-1}y^{-1}x^{-1}\right)^3(xyx)^3\left(x^{-1}y^{-1}\right)^3.$$

在 $B(4)$ 中有关系式:

$$(x,y;5)=\prod_{i=1}^{m} w_i(x,y)^4.$$

在 1981 年, 借助于电子计算机 Havas 得到了 $m=250$ 的这样的关系. 其后 А. В. Корлюков, 把机器和人工计算结合起来, 得到了 $m=28$ 的关系, 而且检验容许不用计算技术. 最小的 $m=m(4)$ 如何以及对于我们感兴趣的情况 $n=5$ 时预计会怎样?

5. 多项式自同构的有限群　假设 G 是所有多项式自同构群 $\mathrm{Aut}\,(\mathbb{C}^n)$ 中的有限子群. G 在 $\mathrm{Aut}\,(\mathbb{C}^n)$ 中与 $\mathrm{GL}(n,\mathbb{C})$ 的一个有限子群共轭吗? 对于 $n=2$ 是正确的 (Гизатуллина-Данилова 定理). 对于 $n\geqslant 3$ 还有一个公开问题 (Furushima Mikio, Tôhoku Math. J. 1983, 35 (3), p.415–424).

6. 单可约群 (或 SR–群, 按照 Е. Вигнера 的术语). 一个有限群 G 称为 SR–群, 如果

$$\sum_{g\in G} f(g)^3=\sum_{g\in G}|C_G(g)|^2,$$

其中 $f(g)=\mathrm{Card}\{x\in G|x^2=g\}$. SR–群的任意两个不可约表示的张量积的展开式系数仅为零和单位, 这对于解释某些物理问题是重要的 (见 Хамермеш М., Теория групп и её применение к физическим проблемам. М.: Мир, 1996). 任何初等交换 2–群, 广义四元数群 Q_{2^n} 和任意二面体群这些例子表明, SR–群的群类不是空集. 我们给出某些解释. 由定义:

$$Q_{2^n}=\left\langle a,b\,\middle|\,a^{2^{(n-1)}}=e,\quad b^2=a^{2^{(n-2)}},\quad ba^i=a^{-i}b\right\rangle,\quad n\geqslant 3.$$

我们看到,

$$Z\left(Q_{2^n}\right)=\left\{e,a^{2^{(n-2)}}\right\}.$$

当 $n=3$ 时, 就得到通常的四元数群. 在 $G=Q_{2^n}$ 中直接计算表明,

$$\sum_g f(g)^3 = \left(2^{n-1}+2\right)^3 + \left(2^{n-2}-1\right)\cdot 2^3$$
$$= \left(2^{n-1}-2\right)\left(2^{n-1}\right)^2 + 2\left(2^n\right)^2 + 2^{n-1}\cdot 4^2 = \sum_g |C_G(g)|^2.$$

类似地, 如果 $G=D_{2n+1}$, 那么

$$\sum_g f(g)^3 = (2n+2)^3 + 2n\cdot 1^3$$
$$= 2^n(2n+1)^2 + 2n(2n+1)^2 + (2n+1)2^2$$
$$= \sum_g |C_G(g)|^2.$$

如果 $G=D_{2n}$, 那么

$$\sum_g f(g)^3 = (2n+2)^3 + (n-1)\cdot 8$$
$$= 2(2\cdot 2n)^2 + (2n-2)(2n)^2 + 2n\cdot 4^2 = \sum_g |C_G(g)|^2.$$

不难验证, 对称群 S_4 是 SR–群, 但 S_5 已经不是, 怎么样一般地用群 G 本身的结构性质的术语来表达群 G 对于 SR–群类的从属关系?

7. 伽罗瓦逆问题 还要讲一讲 "伽罗瓦理论的逆问题". 这里所指的是具有给定伽罗瓦群的有理数域 $\mathbb{Q}$ 的伽罗瓦扩张的构造. D. 希尔伯特是这方面的先驱者: 他的不可约性理论断言, 只要实现给定的群 G 作为函数域 $\mathbb{Q}(x)$ 上扩张的伽罗瓦群就足够了. 既然是这样, 那么就会出现黎曼曲面理论的方法和代数几何的方法. 下面这个出色的定理是后续的转折点.

定理 (沙法列维奇 (И. Р. Шафаревич), 1954 年) *任意有限可解群可作为某一正规扩域 $F/\mathbb{Q}$ 的伽罗瓦群.*

他的方法基本上是数论的方法.

近年来发展的途径是刚性方法, 这在第 5 章已被简要地叙述过, 而且在很大程度上适用于单群或与之接近的群. 刚性, 起初没有运用这个术语, 被 Г. В. Белый (Изв. АН СССР. Сер. матем, 1979, 43(2), 267–276) 首次有效地运用以实现大多数线性群和投射线性群作为域 $\mathbb{Q}$ 的交换扩张 L 的伽罗瓦群 $\mathrm{Gal}(E/L)$. 具有必要根据的刚性和有理性的术语被 J. Thompson 在其文章 (Thompson J, J. Algebra, 1984, 89(2), 337–499) 中引入, 在这篇文章中, 他证明了, 大得出奇的 $M=\mathrm{Gal}(F/\mathbb{Q})$, 对于某些伽罗瓦扩张 $F/\mathbb{Q}$. 大得出奇的 M 本身现今已可靠地进入模形式 (这是由于自己的复不可约特征标的奇异性质) 并且甚至碰到了物理的弦理论. 有好几个专门的会

议就用于这个 M 而召开的 (例如: a) Moonshine, the Monster, and Related Topics: Research Conf., June 1994/Eds Ch. Dong, G. Mason//Contemp. Math.—1996.—No 193; b) Groups, Difference Sets, and the Monster//Eds K. Harada, L. Sohomon et al.—B., N.Y.: de Gruyter, 1996). 有理强刚性的性质在书 [37–39,41] 中被详细讨论. 越来越新的典型单群作为域 $\mathbb{Q}$ 上扩张的伽罗瓦群得到了实现. 但遗憾的是, 远非所有单群都具有有理刚性的性质. 例如, $\mathrm{PSL}(2, 29^2)$ 就不具备这个性质, 虽然众所周知, 这个群是 $\mathbb{Q}$ 上的伽罗瓦群, 而且, 阶为

$$q^2(q-1), \quad (q^2+1), \quad q = 2^{2n+1}$$

的 Suzuki 群 $\mathrm{Sz}(q)$ 也不具有有理刚性的性质, 也不清楚至少对于充分大的 n, 它们是否是 $\mathbb{Q}$ 上的伽罗瓦群. 值得指出的是, $\mathrm{Sz}(q)$ 在单群描写中占有特殊的地位, 因为只有它们的阶不被 3 整除.

伽罗瓦的正问题和其逆问题就下面两方面来说是非常困难的: 对于一个给定的多项式 $f \in \mathbb{Q}[x]$, 算出 $\mathrm{Gal}(f)$; 或反过来, 对于一个给定的伽罗瓦群 G, 甚至对于较小的 $\deg f$ 且 $|G|$ 可以由具备计算机的人们人为地放大, 来寻找相应的多项式. 这方面的工作反映在书 [37] 中. 值得一试的是利用直接计算来证明:

$$\mathrm{Gal}(x^7 - 7x + 3) \cong \mathrm{PSL}(2, 7).$$

困难的原因是因为在某种程度上都是以范德瓦尔登证明的下列事实 (1933 年) 为前提: "几乎所有" n 次多项式有 S_n 作为自己的 $\mathbb{Q}$ 上的伽罗瓦群.

伽罗瓦的逆问题既在我们所熟悉的范围, 又在其它数学理论中广泛出现, 例如, 在伽罗瓦的微分理论中, 这时的代数方程 $f(x) = 0$, 比方说, 由系数属于 $\mathbb{C}(z)$ 的常微分方程所代替. 这里所述问题的详细讨论见: Bourbaki 的讨论班的报告: Van Der Put M., Recent work on differential Galois theory, // Séminaire N. Bourbaki, June 1998, Exp. 849.

习题的答案与提示

字号码 **p.q.r** 表示第 **p** 章 §**q** 习题 **r**.

1.1.3. Q_8 同构于这些矩阵的群.

1.1.4. 不能.

1.2.1. 首先 G 对 H 进行左陪集分解, 然后再按同样的代表元进行右陪集分解.

1.3.1. 取 H 作为点 $1\in\Omega$ 的稳定子群 G_1, 利用分解式 (3) 且令 $\sigma(i)=g_iG_1$.

1.3.3. 将注意力转到群 P 的所有形为 $g=A^iB^iC^i$ 的元, 其中

$$A=\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix},B=\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix},C=\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix};$$

如果 $g\notin Z(P)$, 那么 $C_P(g)=\langle g\rangle Z(G), |G_P(g)|=p^2$.

1.3.4. 如果 $\sigma\in S_n$ 且 $\pi=\pi_1\cdots\pi_m$, 那么

$$\sigma\pi\sigma^{-1}=\sigma\pi_1\sigma^{-1}\cdots\sigma\pi_m\sigma^{-1};$$

进一步, 对于任意长度为 k 的循环置换 $(i_1,i_2,\cdots,i_k)$, 有

$$\sigma(i_1i_2\cdots i_k)\sigma^{-1}=(\sigma(i_1)\sigma(i_2)\cdots\sigma(i_k)).$$

1.3.8. 在和式 $\sum N(g)$ 中每个元 $x\in\Omega$ 被计算 $|St(x)|$ 次, 于是, 与 x 属于同一轨道的元属于 $\sum N(g)$, 等价于说:

$$(G:St(x))\times|St(x)|=|G|.$$

1.3.9. 1) 如果 $D(a)$ 是一个群, 那么 $e\in D(a)$, 于是 $ea=a^{-1}e$, 即 $a^2=e$ 且 $D(a)=C(a)$.

2) 如果 $D(a)$ 是空集, 那么 $E(a)=C(a)\bigcup D(a)$ 是一个群, 于是我们认为 $D(a)$ 是非空集合. 注意到 $xa=a^{-1}x \Longrightarrow a^{-1}x^{-1}=x^{-1}a$. 因此

$$x\in D(a)\Longleftrightarrow x^{-1}\in D(a),\quad xa=a^{-1}x\Longleftrightarrow ax=xa^{-1}.$$

因为 $C(a)$ 和 $D(a)$ 关于逆封闭, 所以集合 $E(a)$ 亦然.

如果 $x,y\in C(a)$, 那么 $xy\in C(a)$. 如果 $x,y\in D(a)$, 那么

$$axy=xa^{-1}y=xya,$$

即 $xy\in C(a)\subset E(a)$. 第三种可能性: $x\in D(a),y\in C(a)$. 在这种情形下,

$$axy=xa^{-1}y=xya^{-1},$$

于是 $xy\in D(a)\subset E(a)$. 剩下注意到 $e\in C(a)\subset E(a)$.

1.4.9. 计算 2 阶元的个数或运用习题 8 的结果.

1.4.12. $aba=ba^2b=ba^{-1}b\Longrightarrow ab^2=aba\cdot a^{-1}b=ba^{-1}b\cdot a^{-1}b=ba^{-1}\cdot aba=b^2a$. 由此推得 $ab=ba$, 从而注意到另外的关系得 $b=e$.

1.4.13. 任意 $n\times n$ 矩阵 $A=(a_{ij})$ 可以写成列向量的形式 $(a_{ij})=(A^{(1)},\cdots,A^{(n)})$, 定义一个映射 $f:S_n\longrightarrow \mathrm{GL}(n)$, 让

$$\pi\mapsto f(\pi)=\left(E^{(\pi_1)},\cdots,E^{(\pi_n)}\right),\qquad (*)$$

这里 $E^{(i)}$ 为单位矩阵 E 的第 i 列. 于是, $f(\pi)$ 是一个 $n\times n$ 矩阵, 其每行和每列有一个元是 1, 其余元素是零 (置换矩阵). 容易理解, $f(\pi)\in \mathrm{GL}(n)$.

设 σ,τ 是任意置换, $\pi=\sigma\tau$ 为它们的乘积. 由定义, 在矩阵 $f(\sigma)=(a_{is})$ 的第 i 行和在矩阵 $f(\tau)=(b_{kl})$ 的第 j 列不同于零的元分别是 $a_{i,\sigma^{-1}i}=1$ 和 $b_{\tau j,j}=1$. 因此, 对于矩阵 $f(\sigma)f(\tau)=(c_{ij})$, 条件 $c_{ij}\neq 0$ 等价于条件: $\sigma_i^{-1}=\tau j$, 即 $i=\sigma\tau j=\pi j$, 而这正说明 $f(\sigma)f(\tau)=f(\sigma\tau)$. 于是 f 是同态.

性质 $\mathrm{Ker}\, f=e$ 显然, 因为由 $(*)$ 式不难发现, $f(\pi)=E\Longrightarrow \pi=e$. 因此 f 是单同态.

最后, 行列式是自己列的一个斜对称函数, 因此 $\det f(\pi)=g\left(E^{(1)},\cdots,E^{(n)}\right)$ 是变量 $E^{(1)},\cdots,E^{(n)}$ 的一个斜对称函数. 由 $(*)$, 以及由 ε_π 的定义及 S_n 作用在 g 上推得:

$$\begin{aligned}\varepsilon_\pi\det f(\pi)&=\varepsilon_\pi\cdot g\left(E^{(1)},\cdots,E^{(n)}\right)=(\pi\circ g)\left(E^{(1)},\cdots,E^{(n)}\right)\\&=g\left(E^{(\pi 1)},\cdots,E^{(\pi n)}\right)=\det\left(E^{(1)},\cdots,E^{(n)}\right)\\&=\det E=1.\end{aligned}$$

于是, $\det f(\pi)=\varepsilon_\pi$.

当 $n=3$ 时,

$$e \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (12) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$
$$(13) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad (23) \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$
$$(123) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad (132) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

2.2.3. 群 S_4 无中心, 而 $\mathrm{SL}(2,3)$ 有阶为 2 的中心. 是的, 群 A_4 与 $\mathrm{PSL}(2,3)$ 同构.

2.2.4. 阶为 $pq\,(p<q)$ 的群 G 一定有一个正规的西罗 q–子群, 因为 $N_q = 1+kq$ 要整除 $|G|$, 而这只可能是 $k=0$. 如果 $N_p=1$, 那么 G 是一个循环群. 当 $N_p = 1+l_p = q$ 时, 那么群 G 是非交换群.

2.2.6. 最有趣的情形是 $|G|=30$. 利用西罗定理直接验证, 至少有一个西罗子群 G_p 是正规的. 否则, $N_5=6, N_3=10$, 从而得到 24 个 5 阶元和 20 个三阶元, 这是不可能的.

2.3.9. 应用基的相容性定理. 在秩相同的情况下, 证明: $\left(F_n^{ab}:A\right)=\det C$, 其中 C 是由 F_n^{ab} 的基到 A 的基的过渡矩阵.

2.4.1. 假设 $\Gamma_t=\log\sigma(t)$. 那么 Γ_t 是 $M_n(\mathbb{R})$ 中的曲线且 $\sigma(t)=\exp(\Gamma_t)$. 如果 $\Gamma_0'=A$, 那么需要证明, Γ_t 是 $M(\mathbb{R})$ 中经过 0 的直线, 即 $\Gamma_t=tA$. 固定 t, 则有

$$\begin{aligned}\Gamma_t' &= \lim_{s\to 0}\frac{\Gamma_{t+s}-\Gamma_t}{s} = \lim_{s\to 0}\frac{\log\sigma(t+s)-\log\sigma(t)}{s}\\ &= \lim_{s\to 0}\frac{\log(\sigma(t)\sigma(s))-\log\sigma(t)}{s},\end{aligned}$$

因为 σ 是一个单参数子群且 $t+s=s+t$. 这表明,

$$\Gamma_t' = \lim_{s\to 0}\frac{\log\sigma(s)}{s} = \Gamma_0'.$$

我们看到, Γ_t' 与 t 无关, 是直线. 于是, $\mathrm{GL}(n,\mathbb{R})$ 的任意切向量等于某一单参数子群在 0 处的导数.

2.5.2. 设 $\mathcal{D}$ 是李代数 $L(G)$ 的一个微分. 让 $c_t=[(\exp(t\mathcal{D}))\mathbf{a},(\exp(t\mathcal{D}))\mathbf{b}]$, 则有:

$$\begin{aligned}\frac{d}{dt}c_t &= [\mathcal{D}(\exp(t\mathcal{D}))\mathbf{a},(\exp(t\mathcal{D}))\mathbf{b}] + [(\exp(t\mathcal{D}))\mathbf{a},\mathcal{D}(\exp(t\mathcal{D}))\mathbf{b}]\\ &= \mathcal{D}[(\exp(t\mathcal{D}))\mathbf{a},(\exp t(\mathcal{D}))\mathbf{b}]\\ &= \mathcal{D}c_t.\end{aligned}$$

但是具有初始条件 $c_0 = [\mathbf{a}, \mathbf{b}]$ 的微分方程

$$\frac{d}{dt}c_t = \mathcal{D}c_t$$

有唯一解:

$$c_t = (\exp(t\mathcal{D}))[\mathbf{a}, \mathbf{b}].$$

我们看到, $\exp(t\mathcal{D})$ 是自同构.

3.1.2. 是.

3.2.1. 对 $e^{i\alpha t}\overline{e^{i\alpha t}}$ 关于 t 求导数, 再令 $t = 0$.

3.3.1. 见第 1 章 §2 定理 2 的证明.

3.3.2. 利用所有 2 阶元的共轭性, 证明它们位于 5 个两两不相交的 (准确地说, 只在 e 点相交) 共轭的 4 阶西罗子群 (见图 6) 中的"一束".

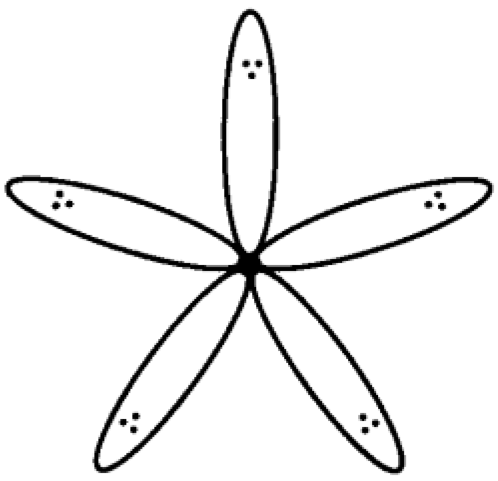


图 6

群 I 共轭地作用在束上. 这个作用是忠实的, 因为 I 是单群 (参见习题 1).

3.3.3. 应用同态定理于 $\Phi : \mathrm{SU}(2) \to \mathrm{SO}(3)$.

3.3.7. 考虑运用项链数计算的结果 (本章开头的问题 2).

3.4.1. 将关系 (4) 和 (5) 重写为形式

$$|G|^{-1}\sum_g \Psi_{jj_0}(g)\varphi_{i_0 i}(g^{-1}) = \delta_{\Phi,\Psi}\frac{\delta_{ji}\delta_{j_0 i_0}}{\chi_\Phi(e)}.$$

在这个等式两边乘上 $\psi_{kj}(h)$ 且关于 j 求和, 注意到等式 $\sum_j \psi_{kj}(h)\psi_{jj_0}(g) = \psi_{kj_0}(hg)$. 在得到的关系式

$$|G|^{-1}\sum_g \psi_{kj_0}(hg)\varphi_{i_0 i}(g^{-1}) = \delta_{\Phi,\Psi}\frac{\psi_{ki}(h)\delta_{j_0 i_0}}{\chi_\Phi(e)}$$

中令 $j_0 = k, i_0 = i$, 然后按 i 和 k 求和而转到特征标.

3.4.3. 假设 Φ 是一个不可约表示, h 是 G 的一个元. 由群的交换性 $\Phi(g)\Phi(h) = \Phi(h)\Phi(g), \forall g \in G$. 在舒尔引理中令 $\sigma = \Phi(h)$, 得到 $\Phi(h) = \lambda_h\mathscr{E}$. 这个等式对于任意 $h \in G$ 成立. 对于不可约的 Φ 只有唯一一种可能性——它是一维的.

3.4.5. 由条件, 对于某个矩阵 $B=(b_{ij})\in \mathrm{GL}(n,\mathbb{C})$ 有 $B\Phi_g B^{-1}=\Psi_g$. 运算 $A\to A^*={}^t\bar{A}$, 适应于 $B\Phi_g=\Psi_g B$, 给出 $\Phi_g^{-1}B^*=B^*\Psi_g^{-1}$, 由此得到 $\Phi_g^{-1}B^*B=B^*B\Phi_g^{-1}$. 根据舒尔引理, $B^*B=\lambda\mathscr{E}$. 进一步, $\lambda=\sum\limits_{k=1}^{n}|b_{ki}|^2=\mu\bar{\mu}$, $\mu\in\mathbb{C}$ 且 $C=\mu^{-1}B$ 是未知的酉矩阵.

3.4.6. 不限制一般性, 我们认为 G 是一个矩阵群: $G\subset \mathrm{GL}(n,\mathbb{C})$, 其中 n 是表示的维数. 令:

$$C(G)=\{M\in M_n(\mathbb{C})|MX=XM,\forall X\in G\}$$

为群 G 在 $M_n(\mathbb{C})$ 中的中心化子. 显然, $C(G)$ 是包含 $Z(G)$ 中的子环. 由舒尔引理, $C(G)$ 中每个不同于零的矩阵非退化. 于是, $C(G)$ 是一个体. 它的中心 K 是一个域且 $Z(G)\subseteq K$. 于是, $Z(G)$ 是域 K 的乘法群的有限子群. 正如在 [BA I] 中所知道的, 这样的子群总是循环的.

3.4.7. 习题解答简述. 只要注意到

$$\chi_\Phi(g)=\mathrm{tr}\Phi_g=\mathrm{tr}\, C_g\Phi_g C_g^{-1}=\mathrm{tr}\Psi_g=\chi_\Psi(g),\quad \forall g\in G,$$

即表示 Φ 和 Ψ 的特征标相等. 现在只需要利用定理 2 的推论.

3.5.2. 由 $a^\tau(\chi_1\chi_2)=a^\tau(\chi_1)a^\tau(\chi_2)$ 推得 a^τ 是群 $\hat{A}$ 的特征标. 因为 $(aa')^\tau=a^\tau(a')^\tau$, 所以 τ 是 A 到 $\hat{\hat{A}}$ 的同态. 又

$$\mathrm{Ker}\,\tau=\{a\in A|a^\tau(\chi)=\chi(a)=1,\forall\chi\in\hat{A}\}\Longrightarrow \mathrm{Ker}\,\tau=e,$$

而 $|\hat{\hat{A}}|=|\hat{A}|=|A|\Longrightarrow\tau$ 是同构.

3.5.7. $5,1,-1,0,0$.

3.6.2. 比较维数, 得到直和空间的展开式

$$P_m=H_m\oplus(x^2+y^2+z^2)H_{m-2}\oplus(x^2+y^2+z^2)^2H_{m-4}\oplus\cdots$$

3.6.4. 由于 SO(3) 是单群, τ 的非平凡性意味着 τ 是忠实 2 维表示. 但是, 正如 §5 第 4 节例 3 所看到的或者由 SU(2) 中有限子群的描写 (见 §3), 就连限制 $\tau|_{\mathbf{O}}$, $\mathbf{O}\cong S_4$ 不可能是忠实的.

4.1.1. 显然, J 是 $Q_M(\mathbb{Z})$ 的真理想. 若 $c/d\notin J$, 则 $c\notin p\mathbb{Z}$, 从而 $d/c\in Q_M(\mathbb{Z})$. 这表明 J 哪怕添加一个元素 c/d 得到的每一个理想都含有 $1=c/d\odot d/c$, 从而和 $Q_M(\mathbb{Z})$ 一致.

4.2.8. 在域 $\mathbb{F}_p$ 的代数闭包 Ω_p 中考虑 1 的一个 8 次本原根 α. 因为 $\alpha^4=-1$, 所以 $\alpha^2+\alpha^{-2}=0$, 此外, $\alpha^5=-\alpha,\alpha^{-5}=-\alpha^{-1}$, 由此得到 $\alpha^5+\alpha^{-5}=-(\alpha+\alpha^{-1})$. 命 $\beta=\alpha+\alpha^{-1}$, 我们将有 $\beta^2=\alpha^2+\alpha^{-2}+2=2$, 于是

$$\begin{aligned}&p\equiv\pm1(\bmod 8)\Longrightarrow\beta^p=\alpha^p+\alpha^{-p}=\alpha+\alpha^{-1}=\beta\Longrightarrow 1\\&=\beta^{p-1}=(\beta^2)^{(p-1)/2}=2^{(p-1)/2}\Longrightarrow\left(\frac{2}{p}\right)=1.\end{aligned}$$

类似地,

$$p \equiv \pm 5 (\mathrm{mod}\, 8) \Longrightarrow \beta^p = \alpha^p + \alpha^{-p} = \alpha^5 + \alpha^{-5} = -(\alpha + \alpha^{-1})$$
$$= -\beta \Longrightarrow -1 = \beta^{p-1} = 2^{(p-1)/2} \Longrightarrow \left(\frac{2}{p}\right) = -1.$$

4.2.9. 若 $n = 1$ 且 $f(x) = \sum\limits_{i=1}^{m} a_i x^i, a_m \neq 0$, 则

$$f(xy) = \sum_{i=1}^{m} a_i x^i y^i = f(x)f(y) = f(x)\left(\sum_{i=1}^{m} a_i y^i\right),$$

其中 x, y 是独立变量. y^m 前面系数的相等表明, $a_m x^m = f(x) a_m$, 从而 $f(x) = x^m$. 现在若在一般情形命 $g(x) = f(x \cdot E)$, 则 $g(xy) = g(x)g(y)$. 由此并由于当 $n = 1$ 时断言正确, 得到 $g(x) = x^s$. 因为 $XX^{\vee} = (\det X) \cdot E$, 所以

$$f(X)f(X^{\vee}) = f((\det X)E) = g(\det X) = (\det X)^s.$$

但是 $f(X), f(X^{\vee})$ 和 $\det X$ 是 $x_{ij}\,(1 \leqslant i, j \leqslant n)$ 的多项式, 并且 $\det X$ 是不可约的 (见 [BA I] 第 5 章 §3 习题 7). 根据关于任意多个变量的多项式环是唯一因子分解整环的定理 4, $f(X) = c(\det X)^m$, 其中 c 是常数, 并且 $f(XY) = f(X)f(Y) \Longrightarrow c^2 = c$, 而因为 $c \neq 0$, 所以 $c = 1$.

4.4.2. 显然, $(1,0)$ 是 $A \oplus A$ 的双边单位元. 命 $e = (0,1)$. 根据定义 $e^2 = -1$. 因为 $(x,0)e = (0,x)$, 所以当将元素 $x \in A$ 和元素 $(x,0) \in A \oplus A$ 等同起来时, 我们得到表达式 $(x,y) = x + ye$. 在 $A \oplus A$ 中的共轭运算由公式 $\overline{(x,y)} = (\overline{x}, -y)$ 给出, 即 $\overline{x + ye} = \overline{x} - ye$. 现在若 $a = x + ye, b = u + ve$, 则

$$\overline{ab} = \overline{xu} + \overline{(ye)u} + \overline{x(ve)} + \overline{(ye)(ve)} = \overline{ux} - \overline{u}(ye) - (ve)\overline{x} + (ve)(ye) = \overline{b}\overline{a}.$$

因此, 共轭运算的定义是合理的. 直接验得性质:

$$ea = \overline{a}e, \quad a(be) = (ba)e.$$

所有这些表明, 如果 A 上的共轭运算不是恒等的, 则代数 A 的双倍是非交换的. 若原有的代数 A 是非交换的, 则其双倍是非结合的. 交换的和结合的代数 A 的双倍是结合的. 特别地, 这些注解指出, 八维凯莱代数 $\mathbb{C}a$ 是非结合的.

4.4.5. 不能. 根据定理 4, 任意两个阶数相同的交换群在 $\mathbb{C}$ 上的群代数的结构是一样的. 当有群环的同构 $(\mathbb{Z}[G] \cong \mathbb{Z}[H])$ 时, 产生了更精细的问题.

4.4.6. 利用定理 3 的推论: $\langle \Phi_g | g \in G \rangle = M_n(\mathbb{C})$. 得到结论, 对任何矩阵 $X \in M_n(\mathbb{C})$ 都有 $\mathrm{tr}(CX) = 0$, 即 $C = 0$.

5.1.4. 考虑多项式 $X^p - a$ 的分裂域 F. 设 $\theta \in F$ 是一个使 $a = \theta^p$ 且 $X^p - a = (X - \theta)^p$ 的根. 现在若 $X^p - a = u(X)v(X)$, 其中 $u(X)$ 是 P 上次数为正数 $m < p$ 的

标准多项式, 则由于 $F(X)$ 是唯一的因子分解环, 应该有等式 $u(X)=(X-\theta)^m$. 特别地, $\theta^m, \theta^p \in P \Longrightarrow \theta \in P$.

5.1.5. 根据前面的习题, 只需证实不可能有等式

$$X^p - Y = \left(X - \frac{g(Y)}{h(Y)}\right)^p,$$

其中 $g, h \in Z_p[Y]$.

5.2.1. 根据 (8), $X^d - 1 = \prod_{e|d} \Phi_e(X)$. 因此

$$X^n - 1 = \left(X^d - 1\right) \prod_{s|n; s\neq d} \Phi_s(X) = \left(X^d - 1\right) \Phi_n(X) \prod_{s|n; s\neq d,n} \Phi_s(X).$$

余下的只要引用 (10).

5.2.2. 因为 $\Phi_n(X)=\prod(X-\varepsilon)$, 其中 ε 跑遍本原根, 所以当 $n>1$ 时所有的 ε 都不等于 1, 因此, 在复数平面上从点 q 到任意一个 ε 的距离都大于从 q 到 1 的距离. 于是 $|\Phi_n(q)|=\prod(q-\varepsilon)>q-1$, 且 $q-1$ 不被 $\Phi_n(q)$ 整除.

5.2.7. 转到方程 $x^2+y^2-z^2=0$, 其中 $x, y, z \in \mathbb{F}_p$. 根据谢瓦莱定理 (见 [BA I] 第 6 章 §1 中的习题 4), 这个方程的解的总数 N 被 p 整除. 设使 $xyz \neq 0$ 的解不存在. 则分别考虑两种情况来计算 N. 若不存在 $a \in \mathbb{F}_p$ 使 $a^2+1=0$, 则解将仅是

$$(0,0,0),(0,n,\pm n),(n,0,\pm n), \quad n=1,2,\cdots,p-1,$$

因此 $N=4p-3 \equiv 0(\bmod p) \Longrightarrow p=3$. 若对某个 $a \in \mathbb{F}_p$, 有 $a^2+1=0$, 则 $N=6p-5 \equiv 0(\bmod p) \Longrightarrow p=5$.

5.2.8. 一般来说, 不是的.

5.3.2. a) A_5; b) S_3; c) S_3; d) Z_4; e) D_4.

5.3.1. 在域 $P(\zeta)$ 上, $\zeta^p=1$, 多项式 $X^p-a \in P[X]$ 或不可约, 或可分解成线性因式的乘积 (其时它的所有的根都是 $P(\zeta)$ 中). 假定后一种情形成立并假定 u 是根当中的一个. 根据定理 4, F/P 将是任何 $F/P \subset P(\zeta)/P$ 的伽罗瓦扩张. 特别地, 元素 u 的极小多项式 f_u 在 $P(u)$ 中分解成线性因式之积. 假定 $u \notin P$, 则 $\deg f_u \geqslant 2$, 我们考虑它的另外一个根 $v \neq u$. 则可选取本原根 $\zeta=u/v \in P(u)$ 且 $P(u)=P(\zeta)$. 这表明, 若 X^p-a 在域 P 中没有根, 则它的所有不可约因式的次数都是 $[P(\zeta):P]$, 即 $[P(\zeta):P]$ 整除素数 p. 但这是不可能的, 这是因为 $1<[P(u):P]=[P(\zeta):P] \leqslant p-1$. 因此, 在 P 中没有根的多项式 X^p-a 在 $P(\zeta)$ 上不可约.

5.4.1. $\theta+1$.

5.5.3. 假定有一个根 α 可以用实根式表示, 我们应该得到结论: 对于剩下的两个实根 β, γ, 这也是对的, 这是因为它们满足系数在域 $P(\alpha)$ 中的二次方程. 根据定理 13, 我们的多项式的分裂域的伽罗瓦群的阶应该是 2 的幂. 但它不是这样的: 3 次不可约多项式的伽罗瓦群的阶被 3 整除.

5.5.4. a) 显然.

b) $\sigma((\mathfrak{L}(v))^n) = (\sigma(\mathfrak{L}(v)))^n = (\zeta\mathfrak{L}(v))^n = \mathfrak{L}(v)^n \Longrightarrow \mathfrak{L}(v) \in P$.

c) 作为 P 上域 F 的基可以取 $(1, u, u^2, \cdots, u^{n-1})$. 命 $u_j = \sigma^j(u)$, 并暂时假定:

$$\mathfrak{L}(u^i) = u_0^i + \zeta^{-1}u_1^i + \cdots + \zeta^{-(n-1)}u_{n-1}^i = 0,$$

其中 $i = 0, 1, \cdots, n-1$. 在这种情形, 矩阵 $\left(u_j^i\right)$ $(0 \leqslant i < j \leqslant n-1)$ 的行将是线性相关的, 而它的行列式 $\det\left(u_j^i\right) = \prod\limits_{k>l}(u_k - u_l)$ 将等于零. 但这不可能, 这是因为所有元素 $u_0, u_1, \cdots, u_{n-1}$ 是两两不相同的.

5.6.2. 事实上, 假定相反. 则 $(g_1, \cdots, g_m) \in \mathcal{S} \Longrightarrow (\sigma g_1, \cdots, \sigma g_m) \in \mathcal{S}$. 因为 G 通过共轭在 $\mathcal{S}$ 上的作用是可迁的, 所以存在 $g \in G$ 使得 $\sigma g_i = g g_i g^{-1}, \forall i$. 但 $\langle g_1, \cdots, g_m \rangle = G$, 从而 σ 是内自同构, 与假定相违.

5.6.3. 为了证明所指出的三元组的强刚性, 最简单的是利用公式 (5) 及我们已知的不可约的复特征标表

	$1A$	$2A$	$3A$	$5A$	$5B$
χ_1	1	1	1	1	1
χ_2	3	-1	0	λ	λ'
χ_3	3	-1	0	λ'	λ
χ_4	4	1	-1	0	0
χ_5	5	1	-1	0	0

在每一种情形计算势 $|\widetilde{\mathcal{S}}|$, 这里 $\lambda = (1+\sqrt{5})/2, \lambda' = \left(1-\sqrt{5}\right)/2$. 计算结果:

$$|\widetilde{\mathcal{S}}(2A, 3A, 5A)| = \frac{60^2}{4\cdot 3\cdot 5}(1+0+0+0+0) = 60,$$
$$|\widetilde{\mathcal{S}}(2A, 5A, 5B)| = \frac{60^2}{4\cdot 5\cdot 5}\left(1+\frac{1}{3}+\frac{1}{3}+0+0\right) = 60,$$
$$|\widetilde{\mathcal{S}}(3A, 5A, 5B)| = \frac{60^2}{3\cdot 5\cdot 5}\left(1+0+0+\frac{1}{4}+0\right) = 60.$$

也容易验证, $\widetilde{\mathcal{S}}$ 中的任意三元组生成 A_5.

5.6.4. 明显的说明: $K_1(z)$ 是整数, 因此 $\overline{K_1(z)} = K_1(z); K_1$ 是中心函数. 更进一步, 像课文中一样论证, 即根据舒尔引理, 我们有等式

$$\frac{1}{|G|}\sum_{x\in G}\Psi_i(xyx^{-1}) = \lambda_i E,$$

其中 Ψ_i 是有特征标 χ_i 的表示, $\lambda_i = \chi_i(y)/\chi_i(e)$. 由方程

$$\frac{1}{|G|}\sum_{x\in G}\Psi_i(xyx^{-1}y^{-1}) = \lambda_i\psi_i(y^{-1})$$

转向迹并对 y 求和，利用正交关系，我们得到

$$\frac{1}{|G|}\sum_{s}^{r} K_1(g_s)\left|g_s^G\right|\chi_i(g_s)=\frac{1}{\chi_i(e)}\sum_{y}\chi_i(y)\overline{\chi_i(y)}=\frac{|G|}{\chi_i(e)}.$$

(g_s 是写成换位子形状的共轭类的代表). 用 $\overline{\chi_i(z)}$来乘并对 i 求和:

$$\frac{1}{|G|}\sum_{s=1}^{r} K_1(g_s)\left|g_s^G\right|\sum_{i=1}^{r}\chi_i(g_s)\overline{\chi_i(z)}=|G|\sum_{i}\frac{\overline{\chi_i(z)}}{\chi_i(e)}.$$

但是在等式左端有 $K_1(z)$, 这是因为若 $g_s^G\neq z^G$, 则

$$\sum_{i=1}^{r}\chi_i(g_s)\overline{\chi_i(z)}=0,$$

而在相反情形则是 $|c(z)|$. 因此,

$$K_1(z)=\overline{K_1(z)}=|G|\sum\frac{\chi_i(z)}{\chi_i(e)}.$$

现在或多或少弄清了是怎样得到 $K_m(z)$ 的表达式的.

教学法方面的意见

因为用于 [BA III] 的讲授和讨论的课时太少, 所以只好以某些框架为目标, 对于该框架尽可能地加上一些细节. 这些框架就叫做教学大纲, 可以根据讲课人的爱好而扩展, 总体上要适合学生的接受能力.

凭借 [BA II] 第 7 章 §1 的材料和根据几何学家的某些需要 (按照他们的要求而引发的), 我们对于线性李群和与之相关的李代数 (第 2 章 §4) 之间关系的叙述是相当提纲式的, 这因为拓扑知识的明显的不足, 贺拉斯可能要不满意了 …… (见 [BA I] 的前言). 但不管怎样, 对照形式 "李代数 → 李群", "多项式 → 它的伽罗瓦群", "任意结合环 → 这个环上的模" 是非常有益的, 因为它们提供了代数统一性的明显的例证, 而代数则是数学的一大领域.

在莫斯科罗蒙诺索夫大学数学力学系, 上面所说用在第三学期的代数构架已经使用好多次了. 伽罗瓦理论已逐渐进入了专题讲座. 实际上, 第 5 章就是为其中的这样一个讲座而写的, 而且这个讲座有效地运用了特征标理论.

考试题 (没有特征标理论)

1. 陪集分解和拉格朗日定理.
2. 循环群的子群.
3. 商群的构造和群同态的基本定理.
4. 第一同构定理.
5. 群的换位子群和交换商群的定理.
6. 中心和关于中心的商群定理.
7. 可解群的概念. 有限 p–群, S_3 和 S_4 的可解性.
8. 直积的同态像定理. 例子.
9. 群的作用: 点的稳定化子, 轨道的长.
10. 共轭作用. 共轭类. 关于有限 p–群的中心的定理.
11. 第一西罗定理 (存在性).
12. 第二西罗定理 (共轭性).
13. 单群 A_5.
14. 单群 SO(3).
15. 有限生成无挠自由交换群. 秩的概念.
16. 有限秩的自由交换群和它的子群的相容基的存在性定理.
17. 作为相容基定理的推论的有限生成交换群的结构定理.
18. 有限交换 p–群的结构定理的直接证明.
19. 有限交换群的基本定理: 不变因子, 初等因子, 例子.
20. 等价的矩阵集合. 舒尔引理和它的推论.
21. 具有有限中心的不可约矩阵群的定理.

22. 有限矩阵群的完全不可约性的 Maschke 定理.
23. 域 $\mathbb{C}$ 上的有限群的矩阵表示. 例子.
24. 表示理论的几何语言. 线性表示的例子. 过渡到矩阵表示.
25. 每个非交换有限群有在任意零特征域上的维数 >1 的不可约表示.
26. 描述有限交换群的所有不可约复表示. 对偶性定理.
27. 有限群的一维复表示个数的定理.
28. 有限群的每个复表示等价于酉表示.
29. n 级线性群在 n 个变量的齐次型上的作用. 线性群的不变量的概念. 例子.
30. 环的理想. 商环.
31. 环的同态基本定理. 主理想环.
32. 域上代数: 结合代数和李代数. 例子. 代数的同态.
33. 多项式代数中的理想. 矩阵代数的单性.
34. 多项式代数的同态像. 代数数域.
35. 多项式的分裂域. 在 $\mathbb{Q}$ 上和 $\mathbb{F}_p$ 上的例子.
36. 任意阶 $q=p^n$ 的有限域的存在.
37. 给定阶的有限域的唯一性.
38. 有限域的自同构.
39. 可除代数. 四元数代数.
40. 弗罗贝尼乌斯定理.

高等代数课程教学大纲 (第三学期, 1995 年)

---

1. 元素的阶和循环群的阶. 同阶的循环群的同构. 循环群的子群的全部描写.

2. 群关于它的子群的左 (右) 陪集的并的分解. 拉格朗日定理和它的推论 (2 小时).

3. 正规子群. 商群. 同态定理和有关同构. 群的直积 (5 小时).

4. 群的作用. 轨道和稳定化子. 共轭元素类和群的中心. 例: S_n 和 A_n (2 小时).

5. 单群的概念. 单群 $A_n, n > 4$ 和 SO(3) (2 小时).

6. 西罗定理 (2 小时).

7. 有限秩的自由交换群和它们的子群. 周期交换群. 有限生成交换群的结构 (4 小时).

8. 环, 代数, 商代数. 多项式在域中的根. 多项式的分裂域. 有限域 (5 小时).

9. 可除代数. 四元数代数. 弗罗贝尼乌斯定理 (2 小时).

10. 群和代数的线性表示. 不变子空间. 不可约和完全可约表示. 矩阵实现. Maschke 定理. 有限交换群的表示 (3 小时).

11. 模. 舒尔引理. 稠密性定理. 单有限维结合代数的构造 (3 小时).

12. 线性李群. 典型群. 李代数. 切李群李代数. 指数映射 (4 小时).

课时总数为 34 (在实际教学中少一些). 必要时部分讲课材料拿到讨论课上.

表示论的例证材料

不接触特征标理论, 可以做许多解释.

问题 1 需要判明: 对称群

$$S_3 = \langle a, b | a^3 = e, b^2 = e, bab^{-1} = a^2 \rangle, \quad a = (123), \quad b = (12),$$

的不可约复表示 $(\Phi, V), \dim V = n > 1$, 精确到等价是唯一的.

令 $\Phi(a) = \mathcal{A}, \Phi(b) = \mathcal{B}$ 且在 V 中选取一组基, 使 $B = \operatorname{diag}(-1, \cdots, -1, 1, \cdots, 1)$. 因为 $Z(S_3) = e$, 所以 B 有 -1 和 $+1$ 作为特征值. 设 $\mathcal{B}v = v$. 显然, $\mathcal{A}v \neq v$, 因为 $n > 1$, 即 $w = \mathcal{A}v - v \neq 0$. 另一方面,

$$(\mathcal{A}^2 + \mathcal{A} + \mathcal{E})w = (\mathcal{A}^2 + \mathcal{A} + \mathcal{E})(\mathcal{A} - \mathcal{E})v = (\mathcal{A}^3 - \mathcal{E})v = 0.$$

我们断定, $\langle w, \mathcal{A}w \rangle$ 是 $\Phi(G)$–不变子空间 (由于不可约性, 它应该等于 V). 事实上, $\mathcal{A}$–不变元被查明. 又

$$\mathcal{B} \cdot \mathcal{A}w = \mathcal{B}(\mathcal{A}^2 - \mathcal{A})v = (\mathcal{A} - \mathcal{A}^2)\mathcal{B}v = (\mathcal{A} - \mathcal{A}^2)v = -\mathcal{A}w,$$
$$\mathcal{B}w = \mathcal{B}\mathcal{A}v - \mathcal{B}v = \mathcal{A}^2\mathcal{B}v - v = (\mathcal{A}^2 - \mathcal{E})v = (\mathcal{A} + \mathcal{E})w.$$

于是在基 $(w, \mathcal{A}w)$ 上有

$$A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}.$$

我们唯一地还原了 (Φ, V). 特别地, $n = 2$.

问题 2 对于四元数群的同样的问题: 有忠实不可约表示 (Φ, V) 和生成 Q_8 且满足下列关系的 V 上的算子 $\mathcal{A}, \mathcal{B}$:

$$\mathcal{A}^4 = \mathcal{E}, \quad \mathcal{B}^2 = \mathcal{A}^2 = -\mathcal{E},$$
$$\mathcal{B}\mathcal{A}\mathcal{B}^{-1} = \mathcal{A}^{-1} = -\mathcal{A}.$$

在 V 中选取一组基, 相对于它有

$$B = \mathrm{diag}(i, \cdots, i, -i, \cdots, -i).$$

因为 Φ 是忠实的, 所以 $+i$ 和 $-i$ 是它的特征值. 设 v 是一个特征向量满足 $\mathcal{B}v = iv$. 关系

$$\mathcal{A}^2 v = -v, \quad \mathcal{B}(\mathcal{A}v) = -\mathcal{A}\mathcal{B}v = -i(\mathcal{A}v)$$

和 (Φ, V) 的不可约性表明: $V = \langle v, \mathcal{A}v \rangle$ 且

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

表示被唯一地还原了.

问题 3 交错群 A_4 由下列表达式定义:

$$A_4 = \langle a, b, c | a^2 = b^2 = (a, b) = e = c^3; cac^{-1} = b, cbc^{-1} = ab \rangle.$$

表示 (Φ, V) 的忠实性和不可约性允许在 V 中选择一组基, 关于它有

$$C = \Phi_c = \mathrm{diag}(1, \cdots, \zeta, \cdots, \zeta^{-1}).$$

不限制一般性, 选择 $0 \neq f \in V$ 使得 $\mathcal{C}f = \zeta f, \zeta \neq 1, \zeta^3 = 1$. 如果 $\mathcal{A}f = f$, 那么

$$\mathcal{B}f = \mathcal{C}\mathcal{A}\mathcal{C}^{-1}f = \mathcal{C}\mathcal{A}\zeta^{-1}f = f$$

这矛盾于 Φ 的不可约性. 于是 $u = \mathcal{A}f - f \neq 0$. 类似地 $v = \mathcal{B}f - f = 0, w = \mathcal{A}\mathcal{B}f - f \neq 0$. 我们有:

$$\mathcal{C}\mathcal{A}f = \mathcal{C}\mathcal{A}\mathcal{C}^{-1}\mathcal{C}f = \mathcal{B}\zeta f = \zeta\mathcal{B}f,$$
$$\mathcal{C}\mathcal{B}f = \mathcal{C}\mathcal{B}\mathcal{C}^{-1}\mathcal{C}f = \mathcal{A}\mathcal{B}\zeta f = \zeta\mathcal{A}\mathcal{B}f,$$
$$\mathcal{C}\mathcal{A}\mathcal{B}f = \mathcal{A}\mathcal{C}f = \zeta\mathcal{A}f.$$

因此 $\mathcal{C}u = \zeta v, \mathcal{C}v = \zeta w, \mathcal{C}w = \zeta u$. 接下来,

$$\mathcal{A}u = -u,$$
$$\mathcal{A}v = \mathcal{A}\mathcal{B}f - \mathcal{A}f = (\mathcal{A}\mathcal{B}f - f) - (\mathcal{A}f - f) = w - u,$$
$$\mathcal{A}w = \mathcal{B}f - \mathcal{A}f = v - u, \quad \mathcal{B}u = \mathcal{A}\mathcal{B}f - \mathcal{B}f = w - v,$$
$$\mathcal{B}v = -v, \quad \mathcal{B}w = \mathcal{A}f - \mathcal{B}f = u - v.$$

我们得到 $\dim V=3$ 及唯一确定的矩阵

$$A=\begin{pmatrix}-1&-1&-1\\0&0&1\\0&1&0\end{pmatrix},\quad B=\begin{pmatrix}0&0&1\\-1&-1&-1\\1&0&0\end{pmatrix},\quad C=\begin{pmatrix}0&0&\zeta\\\zeta&0&0\\0&\zeta&0\end{pmatrix}.$$

名词索引

A

阿廷引理, 182
埃尔米特矩阵, 80
埃尔米特空间, 80
埃尔米特型, 80

B

表示
- ~ 的空间, 71
- ~ 的特征标, 94
- ~ 的维数, 71
- ~ 的张量积, 113
- ~ 的直和, 74
- 不可分 ~, 74
- 不可约 ~, 74
- 代数的 ~, 148
- 等价的 ~, 72
- 对偶 ~, 113
- 交换群的 ~, 103
- 可约 ~, 74
- 逆步 ~, 112, 113
- 平凡 ~, 71
- 群 A_4 的 ~, 106
- 群 A_5 的 ~, 108
- 群 S_4 的 ~, 107
- 群 SU(2) 和 SO(3) 的 ~, 109
- 商 ~, 74
- 四元素群的 ~, 107
- 完全可约 ~, 75
- 线性 ~, 71
- 正则 ~, 77
- 忠实 ~, 71
- 子 ~, 74

不变量
- 二次型的 ~, 118
- 群 S_n 的 ~, 118
- 线性群的 ~, 117, 120

不变因式, 58
不可约多项式, 172
不可约分是出现的重数, 85
布吕阿分解, 40

C

层, 20
超越元素, 166
乘法群 $U(Z_n)$, 134

D

大得出奇的 M, 36
戴德金–阿廷引理, 193

代数, 147
　　～ 的表示, 148
　　～ 的双倍, 160
　　～ 的微分, 161
　　～ A 的维数, 147
　　广义四元数 ～, 159
　　交错 ～, 159
　　结合 ～, 147, 159
　　凯莱 ～, 160
　　可除 ～, 149
　　李 ～, 160
　　群 ～, 152
　　若尔当 ～, 159
　　商 ～, 147
　　四元数 ～, 6
　　中心单 ～, 147
　　子 ～, 147
代数无关, 198
代数整数, 145
单群, 38, 218
　　～ 的分类, 218
第二正交关系, 103
第一同构定理, 23
第一正交关系, 97
定理
　　Maschke ～, 83
　　阿廷 ～, 194
　　阿廷-施赖埃尔 ～, 206
　　别里-汤普森 ～, 211
　　伯恩赛德 ～, 155, 157
　　布饶尔 ～, 192
　　狄利克雷 ～, 200
　　弗罗贝尼乌斯 ～, 149
　　拉格朗日 ～, 12
　　欧拉 ～, 136
　　沙法列维奇 ～, 221
　　施派泽 ～, 203, 204
　　韦德伯恩 ～, 151
　　西罗 ～, 42
　　希尔伯特 ～, 203
　　中国剩余 ～, 135
　　戴德金 ～, 193
　　弗罗贝尼乌斯-施蒂克贝格 ～, 56
对数, 66
多项式的分裂域, 126

E

二次互反律, 138

F

反自同构, 7
范数, 202
分层, 20
分圆多项式, 178, 186
分圆域, 178

G

伽罗瓦对应, 184
伽罗瓦扩张的正规基, 197, 199
伽罗瓦逆问题, 221
高斯整数, 130
根式可解, 207, 209
共轭元素, 102
共轭元素类, 16
　　～ 组的刚性, 211
　　～ 组的强刚性, 211
　　有理 ～, 211
关系, 29
　　～ 的高, 50
　　极小 ～, 50
轨道, 14
　　～ 的长, 15

H

合成列, 41
合成因子, 41
环, 123
　　～ 的理想, 123
　　～ 的整元素, 145
　　多项式 ～, 133

高斯整数 ～, 130
局部 ～, 130
欧几里得 ～, 130
商 ～, 124
剩余类 ～, 124
特征标 ～, 114
唯一因子分解 ～, 133
整元素 ～, 145
主理想 ～, 131
自同态 ～, 140
环的同构定理, 128
换位子, 26

J

角的三等分, 188
极点的重数, 87
极小多项式, 168
极小关系, 188
结构常数, 155
结合代数
～ 的中心, 147
矩阵群中的曲线, 62

K

可分多项式, 172
可解群的步长, 37
可微曲线, 62
空间
不变 ～, 74
稳定 ～, 74
空间的张量积, 113
扩张
～ 的次数, 167
～ 的塔, 167
～ 的本原元素, 166
～ 中元素的范数, 202
～ 中元素的迹, 202
代数 ～, 168
单 ～, 166
伽罗瓦 ～, 183
根式 ～, 207
实根式 ～, 209
循环 ～, 203
有限 ～, 168
正规代数 ～, 183

L

拉普拉斯方程, 68
勒让德符号, 138
理想
～ 的和, 129
～ 的积, 129
～ 的交, 129
多项式环的 ～, 125
极大 ～, 132
素 ～, 130
主 ～, 123
李代数, 160
李群 ～, 65
奇异 ～, 219
李群, 60
～ 的同构, 60
～ 的微分, 64
线性 ～, 60
零化子, 141

M

满同态, 4
幂等元, 156
模, 139
不可约 ～, 142
单 ～, 142
挠 ～, 141
商 ～, 139
循环 ～, 141
有限生成 ～, 141
忠实 ～, 141
周期 ～, 141
子 ～, 139
自由 ～, 143

模理想的剩余类, 124
模同态, 139
默比乌斯反演公式, 176

N

挠, 141

O

欧几里得空间, 80
欧拉函数, 178
欧拉角, 2

P

陪集, 10
　～ 的代表元, 11

Q

切映射, 64
齐次空间, 19
切空间, 63
群, 1
　～ 的积, 27
　～ $U(Z_n)$, 138
　～ 的(内)直积, 28
　～ 的(外)直积, 28
　～ 的基, 49
　～ 的幂指数, 58
　～ 的周期部分, 54
　变换 ～, 14
　初等交换 ～, 59
　单 ～, 38
　单可约 ～, 220
　多项式自同构 ～, 220
　二面体 ～, 31
　二元 ～, 91
　晶体 ～, 109
　可解 ～, 37
　可迁 ～, 18
　空间的运动 ～, 19
　连续 ～, 19
　幂零 ～, 37
　商 ～, 22
　四元数 ～, 33
　四元数代数乘法 ～, 7
　特殊线性 ～, 2
　特征标 ～, 104
　拓扑 ～, 19
　外自同构 ～, 33
　无挠 ～, 49
　辛 ～, 7
　由生成元和关系所定的 ～, 31
　酉 ～, 2
　有限定义的 ～, 31
　有限生成交换 ～, 47
　正则多面体 ～, 88
　正交线性 ～, 2
　自由 ～, 30
　自由交换 ～, 51
　伽罗瓦 ～, 169, 182
群(在集合上的) 作用
　～ 的不变子空间, 73
　～ 的核, 14
　～ 的不变子集, 20
　等价 ～, 20
　共轭 ～, 16
　平移 ～, 17
　忠实的 ～, 14

R

若尔当标准形, 73

S

商群, 21
生成元, 29
　群的 ～, 31
　自由 ～, 30
舒尔引理, 142
数的平方和的分解, 132
四元数
　～ 代数, 6
　共轭 ～, 7

～ 群, 33
～ 的范数, 7
算术级数, 200

T

调和多项式, 110
特征标
～ 表, 103
～ 环, 114
广义 ～, 114
零 ～, 157
体, 6, 149
同构
G – 空间的 ～, 73
分裂域的 ～, 170
同态的微分, 64
同态基本定理, 23
拓扑等价, 3

W

维特公式, 181
稳定化子, 87
无关元素系, 49
无挠交换群, 49

X

下中心列, 37
线性表示, 8
项链, 70
向量
～ 的权, 162
～ 的权的重数, 162
切 ～, 62
最高 ～, 163
旋转的极点, 86

Y

酉算子, 80
有限群的不可约表示, 99
～ 的个数, 99
～ 的维数, 101
有限生成交换群, 47
～ 的基本定理, 57
～ 的结构, 53
～ 的不变量, 58
～ 的初等因子, 58
～ 的型, 58
域, 166
～ 的代数闭包, 172
分圆 ～, 186
完全 ～, 172
有限 ～, 173

Z

正规化子, 16
正规基, 197
正规列, 41
正交算子, 80
正则自同构, 219
置换矩阵, 34
中心函数, 96
中心化子, 15, 16, 142
子表示, 74
子代数, 147
子模
挠 ～, 141
～ 的直和, 129
由集合 T 生成的 ～, 140
子集在群中的指数, 12
子群, 10
博雷尔 ～, 40
挠 ～, 54
导出 ～, 26, 36
共轭 ～, 15
换位 ～, 26, 36
幂单 ～, 40
稳定 ～, 14
西罗 ～, 42
正规 ～, 16
自由基, 143

自由群

　　～ 的秩, 30

　　秩为 n 的 ～, 51

自由生成系, 51

字, 30

　　～ 长, 30

　　空 ～, 30